PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-224236**

(43)Date of publication of application : **17.08.1999**

(51)Int.Cl. G06F 15/00

H04L 9/32

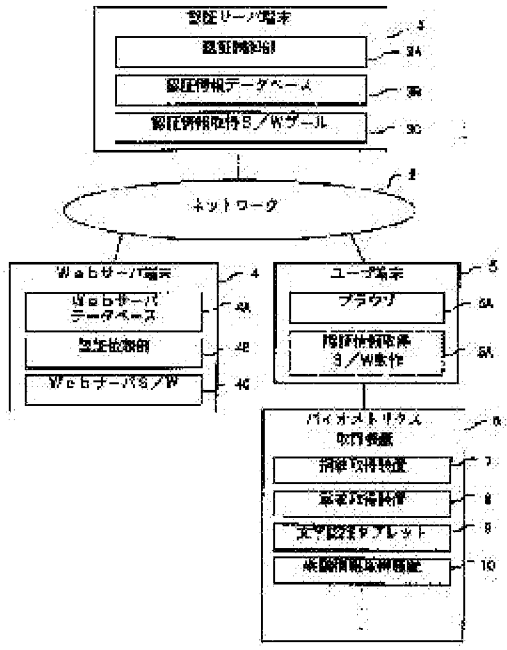
(21)Application number : **10-024225**

(22)Date of filing : **05.02.1998**

(71)Applicant : **MITSUBISHI ELECTRIC CORP**

(72)Inventor : **NAKAMURA HIROSHI**
FUJII TERUKO
SADAKANE TETSUO
BABA YOSHIMASA

(54) REMOTE AUTHENTICATION SYSTEM



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a remote authentication system capable of surely judging the identification an individual and the presence/absence of his access right and substantially improving handleability at the time of authenticating the individual by using obtained biometrics information and key inputted user identification information corresponding to the operation of a prescribed authentication information acquisition software.

SOLUTION: In a Web system 1, authentication is performed by biometrics information. In this case, corresponding to an accessing user terminal 5, a data kind as access information, an authentication request part 4B operated in a Web server terminal 4 as a client of the authentication, the environment of a Web server S/W4C being an application in use and authentication history (authentication time state), an authentication information obtaining S/W for dynamically obtaining the information required for the authentication is selected. Thus, identification of an individual and the presence/absence of his access right are surely judged corresponding to the environment.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] In the remote authentication system which attests the user who a user terminal is connected to a network with an authentication server and an authentication client, respectively, and accesses the above-mentioned authentication client through the above-mentioned user terminal At least 1 or two or more kinds of biometrics acquisition equipments are connected to the above-mentioned user terminal. Or 1 or two or more authentication information acquisition software according to the above-mentioned user are stored. the above-mentioned authentication server -- the above-mentioned user terminal -- and -- Or it responds to actuation of the predetermined authentication information acquisition software according to the above-mentioned user. the above-mentioned user terminal downloaded from the above-mentioned authentication server on the occasion of authentication -- and -- the biometrics information acquired with the above 1 or two or more kinds of biometrics acquisition equipments -- and -- or the remote authentication system characterized by using the user-identification information which it keyed.

[Claim 2] In the remote authentication system which attests the user who a user terminal is connected to a network with an authentication server, respectively, and accesses the above-mentioned user terminal At least 1 or two or more kinds of biometrics acquisition equipments are connected to the above-mentioned user terminal. Or 1 or two or more authentication information acquisition software according to the above-mentioned user are stored. the above-mentioned authentication server -- the above-mentioned user terminal -- and -- Or it responds to actuation of

the predetermined authentication information acquisition software according to the above-mentioned user. the above-mentioned user terminal downloaded from the above-mentioned authentication server on the occasion of authentication -- and -- the biometrics information acquired with the above 1 or two or more kinds of biometrics acquisition equipments -- and -- or the remote authentication system characterized by using the user-identification information which it keyed.
[Claim 3] The remote authentication system according to claim 1 or 2 characterized by having the authentication information acquisition software which has the procedure in which the above-mentioned user chooses whether it uses any they are among two or more above-mentioned biometrics acquisition equipments connected to the above-mentioned user terminal, and inputs as the above-mentioned biometrics information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the system which judges existence of specification of an individual and the access privilege to that individual's information and application intensively at one authentication server terminal by biometrics in a remote authentication system.
[0002]
[Description of the Prior Art] Conventionally, in the information processing system connected to the network, authentication makes [specify an individual and] a judgment of this individual's access permission, and disapproval for a security protection, namely, is required. Moreover, in the cash dispenser of a bank, individual authentication is carried out also at the time of close leaving to the authentication for accessing the dealings information of these individuals, such as specification of an individual and the credit balance, the high research location of whenever [secret], membership system crab, etc.
[0003] Specification of an individual and qualification of rating, i.e., authentication, are carried out with storage of individuals, such as a magnetic card which is the same positioning as an identification card etc. as these authentications, an IC card, and a password, and such combination. however, a password etc. -- fear of oblivion -- it is -- that, as for a magnetic card, an IC card, etc., authentication falls impossible by loss, destruction, etc. **** -- leakage of a theft or password information -- a principal -- there is a problem of except becoming completely with a principal and being attested. Moreover, although it is necessary to attest with a principal certainly in order to keep whenever [secret] high by these, that it is that much hard to remember that a password etc. is complicated or means, such as a one-time password (OTP), are used, it becomes or the authentication actuation itself becomes complicated. To carry out authentication by storage in a wide area (it is used at two or more stores of a bank), it is necessary to manage authentication information intensively, without using a magnetic card etc. furthermore.
[0004]
[Problem(s) to be Solved by the Invention] On the other hand, by the authentication using the biometrics information which is the living body-description of individuals, such as fingerprint information, palm-print information, hand information, and retina information, while canceling complicatedness, it becomes completely, and ** is difficult. When the authentication using biometrics information is required in a wide area, intensive management and authentication are

required also from the same reason as ****, and the field of privacy protection. When carrying out authentication using this biometrics information intensively, it is important to choose the suitable authentication approach with security level (secret level), such as what needs not only every user but authentication, and a location, a system, and to acquire authentication information.
[0005] He is IETF () here. [Internet Engineering] RFC2138 (Remote Authentication Dial InUser Service) registered into RFC (Request ForComment) of Task Force Although the RADIUS server Following RADIUS and a front RFC 2058 are described to be by updating receives the authentication demand of a RADIUS client, performs authentication processing intensively and returns an authentication result An authentication means and authentication information were beforehand decided fixed for every user, and when biometrics information was acquired, there was a problem that an authentication means and authentication information could not be dynamically changed according to the acquisition environment.
[0006] Like the "authentication approach on a network" further shown in JP,9-81518,A as such a conventional example, when the user host has accessed the application server, an application server requests a user's authentication from an authentication server using a fixed authentication means and authentication information, and there is the authentication approach that an authentication result is received.
[0007] Moreover, although biometrics information is effective in identifying an individual, there is also a problem on acquisition sanitarily like [in the case of being accompanied by the problem, and the thing and dysphoria with dirty biometrics acquisition equipment itself of privacy protection].
[0008] In case this invention was made in order to cancel the above trouble, and it attests an individual using biometrics information, it aims at acquiring the remote authentication system and the remote authentication approach which may improve user-friendliness on a target markedly while it can judge specification of an individual and the existence of this individual's access affair certainly.
[0009]
[Means for Solving the Problem] To a network the remote authentication system concerning this invention An authentication server, In the remote authentication system which attests the user to whom it connects, respectively and a user terminal accesses the above-mentioned authentication client through the above-mentioned user terminal with an authentication client At least 1 or two or more kinds of biometrics acquisition equipments are connected to the above-mentioned user terminal. Or 1 or two or more authentication information acquisition software according to the above-mentioned user are stored. the above-mentioned authentication server -- the above-mentioned user terminal -- and -- Or it responds to actuation of the predetermined authentication information acquisition software according to the above-mentioned user. the above-mentioned user terminal downloaded from the above-mentioned authentication server on the occasion of authentication -- and -- the biometrics information acquired with the above 1 or two or more kinds of biometrics acquisition equipments -- and -- or the user-identification information which it keyed is used.
[0010] Moreover, a user terminal is connected to a network with an authentication server, respectively, and the remote authentication system concerning the next invention is set to the remote authentication system which attests the user who accesses the above-mentioned user terminal. At least 1 or two or more kinds of biometrics acquisition equipments are connected to the above-mentioned user terminal. Or 1 or two or more authentication information acquisition software according to the above-mentioned user are stored. the above-mentioned authentication

server -- the above-mentioned user terminal -- and -- Or it responds to actuation of the predetermined authentication information acquisition software according to the above-mentioned user. the above-mentioned user terminal downloaded from the above-mentioned authentication server on the occasion of authentication -- and -- the biometrics information acquired with the above 1 or two or more kinds of biometrics acquisition equipments -- and -- or the user-identification information which it keyed is used.

[0011] The remote authentication system which furthermore starts the next invention is equipped with the authentication information acquisition software which has the procedure in which the above-mentioned user chooses whether it uses any they are among two or more above-mentioned biometrics acquisition equipments connected to the above-mentioned user terminal, and inputs as the above-mentioned biometrics information.

[0012]

[Embodiment of the Invention] With reference to a drawing, the gestalt of implementation of this invention is explained in full detail below.

[0013] The configuration of the gestalt 1 of operation at the time of applying this invention to the Web system 1 at gestalt 1. drawing 1 of operation is shown. The authentication server terminal 3, the authentication client terminal 4 (this example Web server terminal), and user-terminal 5 grade are connected on a network 2. When Web server 4 is accessed through a user terminal 5 from a user by such Web system 1, the user's personal authentication is received from the authentication server terminal 3, and its service is given to a user by the result.

[0014] The authentication server terminals 3 are computer apparatus (what has CPU, memory, a disk, the communications control section, etc. as a configuration is shown hereafter) which store authentication control-section 3A, authentication information database 3B, and authentication information acquisition software pool (software is hereafter described to be S/W) 3C, such as a personal computer and a workstation. Moreover, the Web server terminals 4 are computer apparatus with which Web server database 4A, and authentication request section 4B and Web server S/W4C to be attested [of a user] operate, such as a personal computer and a workstation.

[0015] User-terminal equipment 5 is browser 5A which displays the information on the Web server terminal 4, and computer apparatus with which authentication information acquisition S/W5B operates, such as a personal computer and a workstation. Moreover, biometrics acquisition equipment 6 is connected to user-terminal equipment 5. Biometrics acquisition equipment 6 shows the retina information acquisition equipment 10 grade which acquires the retina information on the body as biometrics information with the fingerprint acquisition equipment 7 which acquires the fingerprint and palm-print information on the body as biometrics information by an image processing etc., palm-print acquisition equipment 8, the character recognition tablet 9 which acquires the hand information which the user drew as biometrics information, an eyegrounds scan, etc.

[0016] The flow of the authentication processing in such a Web system 1 is shown in drawing 2 . Browser 5A which is operating with user-terminal equipment 5 first and which is application explains the case (SP1) where the information on high Web server database 4A of whenever [secrecy / of the Web server terminal 4 / in which a user is the client of authentication] is accessed. Web server S/W4C which is performing the access control of the high information on whenever [secrecy] and which is application needs to perform user authentication, in order for whether this user has an access permission to judge (SP10).

[0017] That is, Web server S/W4C of the Web server terminal 4 notifies being attested [of a user] to authentication request section 4B with Client ID (identifier of the authentication request

section), Application ID (identifier of Web server S/W4C which is the application which needs authentication), and access data classification (secret level of the data which the user has accessed) (SP11). Authentication request section 4B transmits an authentication demand of a user including the above-mentioned information to the authentication server terminal 3.
[0018] Authentication control-section 3A of the authentication server terminal 3 which received the authentication demand of a user chooses authentication information acquisition S/W11 from the authentication client ID, Application ID, and access data classification (SP20). The authentication information acquired, respectively was decided and authentication information acquisition S/W11 also has authentication information acquisition S/W11 which acquires two or more authentication information. Authentication control-section 3A transmits selected authentication information acquisition S/W11 to the Web server terminal 4 which is the client of authentication (SP21).
[0019] Authentication request section 4B of the Web server terminal 4 hands over authentication information acquisition S/W11 transmitted to Web server S/W4C, acquisition of authentication information is directed from a user, and authentication information acquisition S/W11 is transmitted to a user terminal 5 from Web server S/W4C by the directions (SP12).
[0020] As for browser 5A of a user terminal 5, transmitted authentication information acquisition S/W11 operates reception and this authentication information acquisition S/W11 as authentication information S/W5B (SP2). Authentication information S/W acquires the authentication information usually spontaneously used by the conventional computer systems, such as biometrics information, such as acquisition of user ID (an identifier, a firm, a personnel number, affiliation, an address, a telephone, etc. and ID currently assigned for every individual by the system), fingerprint information and palm-print information, hand information, and retina information, a password, and a one-time password. It may operate in harmony with other S/W, such as a driver which acquires authentication information at this time. Authentication information acquisition S/W5B transmits the user ID and authentication information which were acquired to the Web server terminal through browser 5A (SP3).
[0021] Authentication request section 4B of the Web server terminal 4 transmits the user ID and authentication information which were acquired from the user to the authentication server terminal 3 through Web server S/W4C (SP13). Using the user ID and authentication information which were transmitted, authentication control-section 3A of the authentication server terminal 3 carries out user authentication (SP22). Authentication information, such as biometrics information transmitted at this time, is collated with the individual humanity news accumulated in authentication information database 3B of the authentication server terminal 3 from the first. When it is judged as a principal by collating of all the transmitted authentication information, this result is notified to the Web server terminal which is the client of authentication. Moreover, if a collating result is not right, it judges that he is not a principal and notifies at least one of this (SP23).
[0022] Authentication request section 4B of the Web server terminal 4 which is the client of carrier beam authentication about an authentication result notifies the authentication result to Web server S/W4C. Web server S/W4C judges the access permission or disapproval to high information of whenever [secrecy / of a Web server database] to this user by this authentication result (SP14). For example, actuation to user access, such as displaying this extra sensitive information, is performed.
[0023] in addition -- if it enciphers between between a user terminal 5 (authentication information acquisition S/W5B) and the Web server terminal 4, the Web server terminal 4, and

the authentication server terminal 3 (authentication control-section 3A), while being able to keep authentication information secret -- ****** -- a better threat is reducible. moreover -- even if it enciphers between not between individual terminals but the user terminal 5 (authentication information acquisition S/W5B), and the authentication server terminal 3 (authentication control-section 3A) -- the same -- ****** -- a better threat is reducible.

[0024] example 1. -- selection processing of the simple example of a database structure and authentication information acquisition S/W5B is explained here using drawing 3 and drawing 4 . The item of user ID, user level, and authentication information is stored in authentication information database 3B of drawing 3 as information for every individual user. User ID is an identifier, a firm, a personnel number, affiliation, an address, a telephone, etc. and ID currently assigned for every individual by the system. Moreover, user level is an access level to extra sensitive information, and authentication information is biometrics information, such as fingerprint information as authentication information on a collating agency, hand information, and retina information, password information, the information on a one-time password, etc. further.

[0025] The authentication information acquisition S/W11 grade which acquires authentication information acquisition S/W11 which acquires both fingerprint information and retina information, authentication information acquisition S/W11 which acquires two fingerprint information, fingerprint information, and hand information is stored in authentication information acquisition S/W pool 3C of drawing 4 . Moreover, selectable authentication information acquisition S/W11 and data classification corresponding to secret level in authentication information acquisition S/W pool 3C are shown.

[0026] Let the case where the user has accessed information on Web server database 4C of data classification =17 first be an example as explanation of the optional feature of authentication information acquisition S/W11 of the authentication server terminal 3 in this example 1. It is referred to as authentication client ID=15 which are equivalent to the identifier of authentication request section 4B at this time, and is referred to as application ID=25 equivalent to the identifier of Web server S/W4C. Web server S/W4C notifies being attested [of a user] to data classification =17 at authentication request section 4B at the time of access generating. Authentication request section 4B transmits the above-mentioned information, data classification =17, authentication client ID=15, and an authentication demand of the user containing application ID=25 to the authentication server terminal 3. And the authentication server terminal 3 receives the authentication demand including such information.

[0027] Since the data with which authentication control-section 3A of the authentication server terminal 3 was required as the database of authentication information acquisition S/W pool 3C of drawing 4 from the data classification of the received authentication demand are level 2 whenever [secret], they get to know the selectable candidate of with a level of two or more authentication information acquisition S/W11 like a graphic display.

[0028] Some another examples of an authentication information database are explained like drawing 3 using example 2., drawing 5 , and drawing 6 . Here, selectable authentication information acquisition S/W11 for every authentication client ID and every application ID is shown. Authentication control-section 3A of the authentication server terminal 3 gets to know the candidate of authentication information acquisition S/W11 which can choose from the authentication client ID and can be chosen from Application ID using such information. Therefore, A, B, C, D, E, and F become a candidate, C, D, and E become a candidate by the authentication client ID, with Application ID, A, D, E, and F become a candidate and one of D

and the E is eventually chosen by data classification.
[0029] The authentication server terminal 3 from the candidate of this selectable authentication information acquisition S/W chooses selection or S/W regular fixed with means, such as selection or sequential selection, at random. According to environments, such as data classification which is access information, authentication request section 4B which is operating with the equipment which is the client of authentication, and Web server S/W4C which is the application used, an authentication means and authentication information can be flexibly chosen like this example, and the existence of specification of an individual and this individual's access privilege can be certainly judged according to an environment.
[0030] example 3. -- as a following example, user ID is contained in the authentication demand and the case where detail setting out is carried out as the authentication information database of drawing 3 </A> shows drawing 7 is explained. The flow of this processing is shown in drawing 8 which gave the same sign to the corresponding point with drawing 2 . first, the Web server terminal 4 -- user ID (an identifier, a firm, and a personnel number --) ID currently assigned for every individual by affiliation, the address, the telephone, etc. and the system is acquired. The user ID, Client ID (identifier of authentication request section 4B) which were acquired This user's authentication is requested from authentication request section 4B with Application ID (identifier of Web server S/W4C which is the application which needs authentication), and access data classification (secret level of the data which the user has accessed).
[0031] When the authentication information database 3B of drawing 7 is attested with a user's classification (data administrator, general user, etc.), the authentication client ID which can be used, the application ID which can be used, and a principal, the selection situation of authentication information acquisition S/W to the past count of convention authentication and the information for every user individuals, such as a rate of collating, the total count of authentication, and a selection criterion, are added to the authentication information database of drawing 3 as the control information of the application handed over by application and a collating log.
[0032] When user ID is contained in the authentication demand, it chooses in accordance with the selection criterion of the applicable user of drawing 7 . It is user ID =1 as an example, and, as for others, in the case of data classification =17, authentication client ID=15, and application ID=25 as well as a front example, authentication request section 4B transmits an authentication demand of the user who contains user ID =1, data classification =17, authentication client ID=15, and application ID=25 as the above-mentioned information to the authentication server terminal 3.
[0033] And the authentication server terminal 3 receives the authentication demand including such information. A, B, C, D, E, and F become a candidate by data classification like ****, C, D, and E become a candidate by the authentication client ID, by Application ID, A, D, E, and F become a candidate and one of D and the E is chosen eventually. Moreover, user ID = since it is 1, authentication control-section 3A chooses by the total count of authentication. the 1st time of the total count of authentication -- D and the 2nd time -- E3 time -- D and 4timeE .... as -- it chooses. here -- user ID =1 -- the total -- by count =of authentication 20, since it is the 21st time this time, D of authentication information acquisition S/W11 is chosen.
[0034] If the authentication client ID which can be used for authentication information database 3B for every user, and the application ID which can be used have assignment as shown in other examples . and drawing 7 , only while using the authentication client and application which were specified, the access control of sending authentication information acquisition S/W11 to this user

can be realized. Here, since 15 is in the client ID which can be used and 25 is in the application ID which can be used, sending of authentication information acquisition S/W11 is permitted.
[0035] Moreover, the propriety of sending of authentication information acquisition S/W11 can be judged also by user classification shown in drawing 7 . If secret level is furthermore similarly assigned to an authentication client and application with a user, the authentication server terminal 3 can choose authentication information acquisition S/W11 from the level of an authentication client, the level of application, and the level of access data classification at the time of selection of authentication information acquisition S/W11. That is, control which is chosen from authentication information acquisition S/W11 more than the highest level in three, for example can be performed.
[0036] Although it is the same as that of **** after sending of authentication information acquisition S/W11, since user ID is already acquired, the places to which only authentication information is transmitted differ. Moreover, when attested with the principal of drawing 7 , the Web server terminal 4 can also realize a variegated access control using Key-1 which is the control information of the application handed over by application.
[0037] Furthermore, when a selection criterion replaces with this although the selection criterion was the total count of authentication in **** as an example of the rate of collating of drawing 7 , and a selection criterion considers as collating assessment, in with a level of two or more authentication information acquisition S/W11, the highest thing of the past collating assessment is looked for from this user's collating log, and it is chosen. Here, since collating assessment of the last E is the highest, E is chosen.
[0038] Moreover, there is also an example which omits the authentication acquisition S/W transfer to an authentication client from the authentication server terminal 3. When authentication information acquisition S/W is decided by the case of the Web system 1 mentioned above fixed, the Web server terminal 4 of an authentication client acquires authentication information acquisition S/W11 beforehand, and you may make it transmit the authentication information acquisition S/W11 without a transfer of authentication information acquisition S/W to the Web server terminal 4 of an authentication client from the authentication server terminal 3 in it at a user terminal 5 with the Web server terminal 4 which is an authentication client.
[0039] As mentioned above, it sets to this Web system 1. The user who has accessed when attesting using biometrics information, The data classification which is access information, and authentication request section 4B which is operating at the Web server terminal 4 which is the client of authentication, The existence of specification of an individual and this individual's access privilege can be certainly judged according to the environment by choosing authentication information acquisition S/W11 which acquires information dynamically required for authentication according to environments and authentication hysteresis (at the time of authentication condition), such as Web server S/W4C which is the application used.
[0040] gestalt 2. of operation -- the gestalt 1 of operation is simplified in the gestalt 2 of this operation. Drawing 9 which gave the same sign to the corresponding point with drawing 1 has the user terminal which acquires biometrics information, and the same terminal of an authentication client. They are computer apparatus with which local database 5C which there is database retrieval application 5E which performs database retrieval as an example of application to be attested, and database retrieval application 5E uses, authentication request section 5D, and database retrieval application 5E to be attested [of a user] and authentication information acquisition S/W11 operate, such as a personal computer and a workstation. It connects with the

user terminal 5, and it is the completely same configuration as the gestalt 1 of operation mentioned above, and biometrics acquisition equipment 6 is the completely same configuration as the gestalt 1 of the operation which also mentioned the authentication server terminal 3 above.
[0041] In drawing 10 which is fundamentally the same as the gestalt 1 of above-mentioned operation, and gave the same sign to the corresponding point with drawing 2 and drawing 8 database retrieval application 5E In case it accesses to the extra sensitive information of local database 5C, (SP5), User ID (an identifier, a firm, a personnel number, affiliation, an address, a telephone, etc. and ID currently assigned for every individual by the system) is acquired first (SP6). The user ID, Client ID (identifier of authentication request section 5D) which were acquired This user's authentication is requested from authentication request section 5D with Application ID (identifier of database retrieval application 5E which is the application which needs authentication), and access data classification (secret level of the data which the user has accessed) (SP7).
[0042] Actuation of the authentication server terminal 3 is the same as the gestalt 1 of operation, authentication processing is performed, and authentication request section 5D of the user terminal 5 which is the client of carrier beam authentication about an authentication result notifies the authentication result to database retrieval application 5E. Database retrieval application 5E judges whether access to the high information on whenever [secrecy / of local database 5C] is permitted to this user by this authentication result (SP8). For example, actuation to user access, such as displaying this extra sensitive information, is performed. According to such a configuration, a user terminal 5 can acquire the same effectiveness as the gestalt 1 of operation mentioned above in the configuration which advances an authentication request.
[0043] gestalt 3. of operation -- with the gestalt 3 of this operation, in drawing 2 and drawing 11 which gave the same sign to the corresponding point with drawing 8 , when the personal authentication information specified by authentication information acquisition S/W11 transmitted from the authentication server 3 does not suit a user's intention, the procedure (SP2B, SP12A) in which a user refuses applicable authentication information acquisition S/W is shown. The authentication server terminal 3 with which acquisition was refused reselects other authentication information acquisition S/W (SP20A). However, it is the case where there is other authentication information acquisition S/W which can reselect as mentioned above about drawing 4 .
[0044] When accompanied by a thing and dysphoria with the specified biometrics acquisition equipment 6 dirty when using biometrics as individual authentication information, a user does refusal. Although biometrics is effective in identifying an individual, the problem of privacy protection and the opportunity for a user to also refuse or change a sanitary problem for a certain reason are indispensable as mentioned above.
[0045] Moreover, also when biometrics acquisition equipment 6 cannot trust it in security, even if there is the intention to say that he wants to specify alternative means, such as a one-time password (OTP), even if complicated [other than biometrics information] and it follows the intention of refusal of a user or modification, the effectiveness that the existence of specification of an individual and this individual's access privilege can be certainly judged according to the environment can acquire by choosing authentication information acquisition S/W which acquires information dynamically required for authentication.
[0046] As a means to acquire the same effectiveness as the gestalt 3 of gestalt 4. implementation of operation, the optional feature of acquisition authentication information is included in authentication information acquisition S/W of the gestalten 1 and 2 of operation itself. In the

example of the gestalt 1 of operation, what carries out authentication implementation for the fingerprint and hand information on D, and the thing to attest only with the fingerprint of E can be chosen as authentication information acquisition S/W which can be chosen. At this time, the places to which authentication information acquisition S/W which an authentication server combines with the authentication information acquisition function of D and E both is transmitted differ.

[0047] The configuration and operations sequence of Web system 1 the very thing are the same as that of the gestalten 1 and 2 of operation. The screen image of authentication information acquisition S/W by the side of a user is shown in drawing 12 . A user chooses either from D/E and acquires his own [an authentication means and] authentication information. If it chooses any of the selection carbon buttons 12A and 12B of a screen they are, authentication information acquisition S/W will operate, and authentication information chosen actually is acquired. At the authentication server terminal 3, with the classification of the sent authentication information, it can judge whether it can attest in the group of the sent information, and the same effectiveness as the gestalt 3 of operation can be acquired.

[0048] Although the authentication information acquired by authentication information acquisition S/W was determined with the gestalten 1-4 of the gestalt 5. above-mentioned operation of operation, it is good even if like [which the authentication information acquired not on authentication information acquisition S/W but on a screen is shown]. For example, at the time of the count of authentication of the detail database of the gestalt 1 of operation, it is displayed that fingerprint information and hand information are sent to a screen. Thereby, a user operates the software which acquires authentication information spontaneously according to the displayed content, and sends the acquired authentication information to the authentication server terminal 3.

[0049] Moreover, you may make it display that the authentication information which was not shown concretely but was beforehand decided by the display is sent. In this case, the software with which a user acquires authentication information for all the authentication information beforehand notified in advance by storage of a user from the manager etc. to the user separately spontaneously is operated, and the acquired authentication information is sent to an authentication server. If it does in this way, the same effectiveness as the gestalt 1 of above-mentioned operation is realizable, but in a display, since a means to acquire serves as treatment like a password when sending the authentication information which was not shown concretely but was decided beforehand, security can be improved much more.

[0050] In addition, in the gestalten 1-4 of above-mentioned operation, in the Web server terminal 4, although the case where a user's personal authentication was performed was described, it is widely applicable [this invention] to the general control unit which needs a user's personal authentication like the close leaving terminal unit connected not only to this but to the network.

[0051]

[Effect of the Invention] As above-mentioned, according to this invention, in case it attests using biometrics information, although an authentication server chooses biometrics acquisition equipment and authentication information freely and acquires them according to the acquisition environment of a user's biometrics information, it is made, and can realize the remote authentication system which can judge the existence of specification of a user and that user's access privilege certainly in this way.

[0052] Moreover, a user can change and refuse the authentication information acquired when there is dissatisfaction about acquisition of the specified authentication information, and even

when the equipment which acquires the case where biometrics acquisition equipment is accompanied by displeasure by dirty **, and biometrics information is not reliable, he can judge the existence of specification of a user and the user's access privilege certainly certain in this way with an alternative means.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the system which judges existence of specification of an individual and the access privilege to that individual's information and application intensively at one authentication server terminal by biometrics in a remote authentication system.

PRIOR ART

[Description of the Prior Art] Conventionally, in the information processing system connected to the network, authentication makes [specify an individual and] a judgment of this individual's access permission, and disapproval for a security protection, namely, is required. Moreover, in the cash dispenser of a bank, individual authentication is carried out also at the time of close leaving to the authentication for accessing the dealings information of these individuals, such as specification of an individual and the credit balance, the high research location of whenever [secret], membership system crab, etc.

[0003] Specification of an individual and qualification of rating, i.e., authentication, are carried out with storage of individuals, such as a magnetic card which is the same positioning as an identification card etc. as these authentications, an IC card, and a password, and such combination. however, a password etc. -- fear of oblivion -- it is -- that, as for a magnetic card, an IC card, etc., authentication falls impossible by loss, destruction, etc. **** -- leakage of a theft or password information -- a principal -- there is a problem of except becoming completely with a principal and being attested. Moreover, although it is necessary to attest with a principal certainly in order to keep whenever [secret] high by these, that it is that much hard to remember that a password etc. is complicated or means, such as a one-time password (OTP), are used, it becomes or the authentication actuation itself becomes complicated. To carry out authentication by storage in a wide area (it is used at two or more stores of a bank), it is necessary to manage authentication information intensively, without using a magnetic card etc. furthermore.

EFFECT OF THE INVENTION

[Effect of the Invention] As above-mentioned, according to this invention, in case it attests using biometrics information, although an authentication server chooses biometrics acquisition equipment and authentication information freely and acquires them according to the acquisition environment of a user's biometrics information, it is made, and can realize the remote authentication system which can judge the existence of specification of a user and that user's access privilege certainly in this way.

[0052] Moreover, a user can change and refuse the authentication information acquired when there is dissatisfaction about acquisition of the specified authentication information, and even when the equipment which acquires the case where biometrics acquisition equipment is accompanied by displeasure by dirty **, and biometrics information is not reliable, he can judge

the existence of specification of a user and the user's access privilege certainly certain in this way with an alternative means.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] On the other hand, by the authentication using the biometrics information which is the living body-description of individuals, such as fingerprint information, palm-print information, hand information, and retina information, while canceling complicatedness, it becomes completely, and ** is difficult. When the authentication using biometrics information is required in a wide area, intensive management and authentication are required also from the same reason as ****, and the field of privacy protection. When carrying out authentication using this biometrics information intensively, it is important to choose the suitable authentication approach with security level (secret level), such as what needs not only every user but authentication, and a location, a system, and to acquire authentication information.
[0005] He is IETF () here. [Internet Engineering] RFC2138 (Remote Authentication Dial InUser Service) registered into RFC (Request ForComment) of Task Force Although the RADIUS server Following RADIUS and a front RFC 2058 are described to be by updating receives the authentication demand of a RADIUS client, performs authentication processing intensively and returns an authentication result An authentication means and authentication information were beforehand decided fixed for every user, and when biometrics information was acquired, there was a problem that an authentication means and authentication information could not be dynamically changed according to the acquisition environment.
[0006] Like the "authentication approach on a network" further shown in JP,9-81518,A as such a conventional example, when the user host has accessed the application server, an application server requests a user's authentication from an authentication server using a fixed authentication means and authentication information, and there is the authentication approach that an authentication result is received.
[0007] Moreover, although biometrics information is effective in identifying an individual, there is also a problem on acquisition sanitarily like [in the case of being accompanied by the problem, and the thing and dysphoria with dirty biometrics acquisition equipment itself of privacy protection].
[0008] In case this invention was made in order to cancel the above trouble, and it attests an individual using biometrics information, it aims at acquiring the remote authentication system and the remote authentication approach which may improve user-friendliness on a target markedly while it can judge specification of an individual and the existence of this individual's access affair certainly.

MEANS

[Means for Solving the Problem] To a network the remote authentication system concerning this invention An authentication server, In the remote authentication system which attests the user to whom it connects, respectively and a user terminal accesses the above-mentioned authentication client through the above-mentioned user terminal with an authentication client At least 1 or two or more kinds of biometrics acquisition equipments are connected to the above-mentioned user terminal. Or 1 or two or more authentication information acquisition software according to the above-mentioned user are stored. the above-mentioned authentication server -- the above-

mentioned user terminal -- and -- Or it responds to actuation of the predetermined authentication information acquisition software according to the above-mentioned user. the above-mentioned user terminal downloaded from the above-mentioned authentication server on the occasion of authentication -- and -- the biometrics information acquired with the above 1 or two or more kinds of biometrics acquisition equipments -- and -- or the user-identification information which it keyed is used.

[0010] Moreover, a user terminal is connected to a network with an authentication server, respectively, and the remote authentication system concerning the next invention is set to the remote authentication system which attests the user who accesses the above-mentioned user terminal. At least 1 or two or more kinds of biometrics acquisition equipments are connected to the above-mentioned user terminal. Or 1 or two or more authentication information acquisition software according to the above-mentioned user are stored. the above-mentioned authentication server -- the above-mentioned user terminal -- and -- Or it responds to actuation of the predetermined authentication information acquisition software according to the above-mentioned user. the above-mentioned user terminal downloaded from the above-mentioned authentication server on the occasion of authentication -- and -- the biometrics information acquired with the above 1 or two or more kinds of biometrics acquisition equipments -- and -- or the user-identification information which it keyed is used.

[0011] The remote authentication system which furthermore starts the next invention is equipped with the authentication information acquisition software which has the procedure in which the above-mentioned user chooses whether it uses any they are among two or more above-mentioned biometrics acquisition equipments connected to the above-mentioned user terminal, and inputs as the above-mentioned biometrics information.

[0012]

[Embodiment of the Invention] With reference to a drawing, the gestalt of implementation of this invention is explained in full detail below.

[0013] The configuration of the gestalt 1 of operation at the time of applying this invention to the Web system 1 at gestalt 1. drawing 1 of operation is shown. The authentication server terminal 3, the authentication client terminal 4 (this example Web server terminal), and user-terminal 5 grade are connected on a network 2. When Web server 4 is accessed through a user terminal 5 from a user by such Web system 1, the user's personal authentication is received from the authentication server terminal 3, and its service is given to a user by the result.

[0014] The authentication server terminals 3 are computer apparatus (what has CPU, memory, a disk, the communications control section, etc. as a configuration is shown hereafter) which store authentication control-section 3A, authentication information database 3B, and authentication information acquisition software pool (software is hereafter described to be S/W) 3C, such as a personal computer and a workstation. Moreover, the Web server terminals 4 are computer apparatus with which Web server database 4A, and authentication request section 4B and Web server S/W4C to be attested [of a user] operate, such as a personal computer and a workstation.

[0015] User-terminal equipment 5 is browser 5A which displays the information on the Web server terminal 4, and computer apparatus with which authentication information acquisition S/W5B operates, such as a personal computer and a workstation. Moreover, biometrics acquisition equipment 6 is connected to user-terminal equipment 5. Biometrics acquisition equipment 6 shows the retina information acquisition equipment 10 grade which acquires the retina information on the body as biometrics information with the fingerprint acquisition equipment 7 which acquires the fingerprint and palm-print information on the body as biometrics

information by an image processing etc., palm-print acquisition equipment 8, the character recognition tablet 9 which acquires the hand information which the user drew as biometrics information, an eyegrounds scan, etc.

[0016] The flow of the authentication processing in such a Web system 1 is shown in drawing 2 . Browser 5A which is operating with user-terminal equipment 5 first and which is application explains the case (SP1) where the information on high Web server database 4A of whenever [secrecy / of the Web server terminal 4 / in which a user is the client of authentication] is accessed. Web server S/W4C which is performing the access control of the high information on whenever [secrecy] and which is application needs to perform user authentication, in order for whether this user has an access permission to judge (SP10).

[0017] That is, Web server S/W4C of the Web server terminal 4 notifies being attested [of a user] to authentication request section 4B with Client ID (identifier of the authentication request section), Application ID (identifier of Web server S/W4C which is the application which needs authentication), and access data classification (secret level of the data which the user has accessed) (SP11). Authentication request section 4B transmits an authentication demand of a user including the above-mentioned information to the authentication server terminal 3.

[0018] Authentication control-section 3A of the authentication server terminal 3 which received the authentication demand of a user chooses authentication information acquisition S/W11 from the authentication client ID, Application ID, and access data classification (SP20). The authentication information acquired, respectively was decided and authentication information acquisition S/W11 also has authentication information acquisition S/W11 which acquires two or more authentication information. Authentication control-section 3A transmits selected authentication information acquisition S/W11 to the Web server terminal 4 which is the client of authentication (SP21).

[0019] Authentication request section 4B of the Web server terminal 4 hands over authentication information acquisition S/W11 transmitted to Web server S/W4C, acquisition of authentication information is directed from a user, and authentication information acquisition S/W11 is transmitted to a user terminal 5 from Web server S/W4C by the directions (SP12).

[0020] As for browser 5A of a user terminal 5, transmitted authentication information acquisition S/W11 operates reception and this authentication information acquisition S/W11 as authentication information S/W5B (SP2). Authentication information S/W acquires the authentication information usually spontaneously used by the conventional computer systems, such as biometrics information, such as acquisition of user ID (an identifier, a firm, a personnel number, affiliation, an address, a telephone, etc. and ID currently assigned for every individual by the system), fingerprint information and palm-print information, hand information, and retina information, a password, and a one-time password. It may operate in harmony with other S/W, such as a driver which acquires authentication information at this time. Authentication information acquisition S/W5B transmits the user ID and authentication information which were acquired to the Web server terminal through browser 5A (SP3).

[0021] Authentication request section 4B of the Web server terminal 4 transmits the user ID and authentication information which were acquired from the user to the authentication server terminal 3 through Web server S/W4C (SP13). Using the user ID and authentication information which were transmitted, authentication control-section 3A of the authentication server terminal 3 carries out user authentication (SP22). Authentication information, such as biometrics information transmitted at this time, is collated with the individual humanity news accumulated in authentication information database 3B of the authentication server terminal 3 from the first.

When it is judged as a principal by collating of all the transmitted authentication information, this result is notified to the Web server terminal which is the client of authentication. Moreover, if a collating result is not right, it judges that he is not a principal and notifies at least one of this (SP23).

[0022] Authentication request section 4B of the Web server terminal 4 which is the client of carrier beam authentication about an authentication result notifies the authentication result to Web server S/W4C. Web server S/W4C judges the access permission or disapproval to high information of whenever [secrecy / of a Web server database] to this user by this authentication result (SP14). For example, actuation to user access, such as displaying this extra sensitive information, is performed.

[0023] in addition -- if it enciphers between between a user terminal 5 (authentication information acquisition S/W5B) and the Web server terminal 4, the Web server terminal 4, and the authentication server terminal 3 (authentication control-section 3A), while being able to keep authentication information secret -- ****** -- a better threat is reducible. moreover -- even if it enciphers between not between individual terminals but the user terminal 5 (authentication information acquisition S/W5B), and the authentication server terminal 3 (authentication control-section 3A) -- the same -- ****** -- a better threat is reducible.

[0024] example 1. -- selection processing of the simple example of a database structure and authentication information acquisition S/W5B is explained here using drawing 3 and drawing 4 . The item of user ID, user level, and authentication information is stored in authentication information database 3B of drawing 3 as information for every individual user. User ID is an identifier, a firm, a personnel number, affiliation, an address, a telephone, etc. and ID currently assigned for every individual by the system. Moreover, user level is an access level to extra sensitive information, and authentication information is biometrics information, such as fingerprint information as authentication information on a collating agency, hand information, and retina information, password information, the information on a one-time password, etc. further.

[0025] The authentication information acquisition S/W11 grade which acquires authentication information acquisition S/W11 which acquires both fingerprint information and retina information, authentication information acquisition S/W11 which acquires two fingerprint information, fingerprint information, and hand information is stored in authentication information acquisition S/W pool 3C of drawing 4 . Moreover, selectable authentication information acquisition S/W11 and data classification corresponding to secret level in authentication information acquisition S/W pool 3C are shown.

[0026] Let the case where the user has accessed information on Web server database 4C of data classification =17 first be an example as explanation of the optional feature of authentication information acquisition S/W11 of the authentication server terminal 3 in this example 1. It is referred to as authentication client ID=15 which are equivalent to the identifier of authentication request section 4B at this time, and is referred to as application ID=25 equivalent to the identifier of Web server S/W4C. Web server S/W4C notifies being attested [of a user] to data classification =17 at authentication request section 4B at the time of access generating. Authentication request section 4B transmits the above-mentioned information, data classification =17, authentication client ID=15, and an authentication demand of the user containing application ID=25 to the authentication server terminal 3. And the authentication server terminal 3 receives the authentication demand including such information.

[0027] Since the data with which authentication control-section 3A of the authentication server

terminal 3 was required as the database of authentication information acquisition S/W pool 3C of drawing 4 from the data classification of the received authentication demand are level 2 whenever [secret], they get to know the selectable candidate of with a level of two or more authentication information acquisition S/W11 like a graphic display.
[0028] Some another examples of an authentication information database are explained like drawing 3 using example 2., drawing 5 , and drawing 6 . Here, selectable authentication information acquisition S/W11 for every authentication client ID and every application ID is shown. Authentication control-section 3A of the authentication server terminal 3 gets to know the candidate of authentication information acquisition S/W11 which can choose from the authentication client ID and can be chosen from Application ID using such information. Therefore, A, B, C, D, E, and F become a candidate, C, D, and E become a candidate by the authentication client ID, with Application ID, A, D, E, and F become a candidate and one of D and the E is eventually chosen by data classification.
[0029] The authentication server terminal 3 from the candidate of this selectable authentication information acquisition S/W chooses selection or S/W regular fixed with means, such as selection or sequential selection, at random. According to environments, such as data classification which is access information, authentication request section 4B which is operating with the equipment which is the client of authentication, and Web server S/W4C which is the application used, an authentication means and authentication information can be flexibly chosen like this example, and the existence of specification of an individual and this individual's access privilege can be certainly judged according to an environment.
[0030] example 3. -- as a following example, user ID is contained in the authentication demand and the case where detail setting out is carried out as the authentication information database of drawing 3 shows drawing 7 is explained. The flow of this processing is shown in drawing 8 which gave the same sign to the corresponding point with drawing 2 . first, the Web server terminal 4 -- user ID (an identifier, a firm, and a personnel number --) ID currently assigned for every individual by affiliation, the address, the telephone, etc. and the system is acquired. The user ID, Client ID (identifier of authentication request section 4B) which were acquired This user's authentication is requested from authentication request section 4B with Application ID (identifier of Web server S/W4C which is the application which needs authentication), and access data classification (secret level of the data which the user has accessed).
[0031] When the authentication information database 3B of drawing 7 is attested with a user's classification (data administrator, general user, etc.), the authentication client ID which can be used, the application ID which can be used, and a principal, the selection situation of authentication information acquisition S/W to the past count of convention authentication and the information for every user individuals, such as a rate of collating, the total count of authentication, and a selection criterion, are added to the authentication information database of drawing 3 as the control information of the application handed over by application and a collating log.
[0032] When user ID is contained in the authentication demand, it chooses in accordance with the selection criterion of the applicable user of drawing 7 . It is user ID =1 as an example, and, as for others, in the case of data classification =17, authentication client ID=15, and application ID=25 as well as a front example, authentication request section 4B transmits an authentication demand of the user who contains user ID =1, data classification =17, authentication client ID=15, and application ID=25 as the above-mentioned information to the authentication server terminal 3.

[0033] And the authentication server terminal 3 receives the authentication demand including such information. A, B, C, D, E, and F become a candidate by data classification like ****, C, D, and E become a candidate by the authentication client ID, by Application ID, A, D, E, and F become a candidate and one of D and the E is chosen eventually. Moreover, user ID = since it is 1, authentication control-section 3A chooses by the total count of authentication. the 1st time of the total count of authentication -- D and the 2nd time -- E3 time -- D and 4timeE .... as -- it chooses. here -- user ID =1 -- the total -- by count =of authentication 20, since it is the 21st time this time, D of authentication information acquisition S/W11 is chosen.
[0034] If the authentication client ID which can be used for authentication information database 3B for every user, and the application ID which can be used have assignment as shown in other examples . and drawing 7 , only while using the authentication client and application which were specified, the access control of sending authentication information acquisition S/W11 to this user can be realized. Here, since 15 is in the client ID which can be used and 25 is in the application ID which can be used, sending of authentication information acquisition S/W11 is permitted.
[0035] Moreover, the propriety of sending of authentication information acquisition S/W11 can be judged also by user classification shown in drawing 7 . If secret level is furthermore similarly assigned to an authentication client and application with a user, the authentication server terminal 3 can choose authentication information acquisition S/W11 from the level of an authentication client, the level of application, and the level of access data classification at the time of selection of authentication information acquisition S/W11. That is, control which is chosen from authentication information acquisition S/W11 more than the highest level in three, for example can be performed.
[0036] Although it is the same as that of **** after sending of authentication information acquisition S/W11, since user ID is already acquired, the places to which only authentication information is transmitted differ. Moreover, when attested with the principal of drawing 7 , the Web server terminal 4 can also realize a variegated access control using Key-1 which is the control information of the application handed over by application.
[0037] Furthermore, when a selection criterion replaces with this although the selection criterion was the total count of authentication in **** as an example of the rate of collating of drawing 7 , and a selection criterion considers as collating assessment, in with a level of two or more authentication information acquisition S/W11, the highest thing of the past collating assessment is looked for from this user's collating log, and it is chosen. Here, since collating assessment of the last E is the highest, E is chosen.
[0038] Moreover, there is also an example which omits the authentication acquisition S/W transfer to an authentication client from the authentication server terminal 3. When authentication information acquisition S/W is decided by the case of the Web system 1 mentioned above fixed, the Web server terminal 4 of an authentication client acquires authentication information acquisition S/W11 beforehand, and you may make it transmit the authentication information acquisition S/W11 without a transfer of authentication information acquisition S/W to the Web server terminal 4 of an authentication client from the authentication server terminal 3 in it at a user terminal 5 with the Web server terminal 4 which is an authentication client.
[0039] As mentioned above, it sets to this Web system 1. The user who has accessed when attesting using biometrics information, The data classification which is access information, and authentication request section 4B which is operating at the Web server terminal 4 which is the client of authentication, The existence of specification of an individual and this individual's

access privilege can be certainly judged according to the environment by choosing authentication information acquisition S/W11 which acquires information dynamically required for authentication according to environments and authentication hysteresis (at the time of authentication condition), such as Web server S/W4C which is the application used.
[0040] gestalt 2. of operation -- the gestalt 1 of operation is simplified in the gestalt 2 of this operation. Drawing 9 which gave the same sign to the corresponding point with drawing 1 has the user terminal which acquires biometrics information, and the same terminal of an authentication client. They are computer apparatus with which local database 5C which there is database retrieval application 5E which performs database retrieval as an example of application to be attested, and database retrieval application 5E uses, authentication request section 5D, and database retrieval application 5E to be attested [of a user] and authentication information acquisition S/W11 operate, such as a personal computer and a workstation. It connects with the user terminal 5, and it is the completely same configuration as the gestalt 1 of operation mentioned above, and biometrics acquisition equipment 6 is the completely same configuration as the gestalt 1 of the operation which also mentioned the authentication server terminal 3 above.
[0041] In drawing 10 which is fundamentally the same as the gestalt 1 of above-mentioned operation, and gave the same sign to the corresponding point with drawing 2 and drawing 8 database retrieval application 5E In case it accesses to the extra sensitive information of local database 5C, (SP5), User ID (an identifier, a firm, a personnel number, affiliation, an address, a telephone, etc. and ID currently assigned for every individual by the system) is acquired first (SP6). The user ID, Client ID (identifier of authentication request section 5D) which were acquired This user's authentication is requested from authentication request section 5D with Application ID (identifier of database retrieval application 5E which is the application which needs authentication), and access data classification (secret level of the data which the user has accessed) (SP7).
[0042] Actuation of the authentication server terminal 3 is the same as the gestalt 1 of operation, authentication processing is performed, and authentication request section 5D of the user terminal 5 which is the client of carrier beam authentication about an authentication result notifies the authentication result to database retrieval application 5E. Database retrieval application 5E judges whether access to the high information on whenever [secrecy / of local database 5C] is permitted to this user by this authentication result (SP8). For example, actuation to user access, such as displaying this extra sensitive information, is performed. According to such a configuration, a user terminal 5 can acquire the same effectiveness as the gestalt 1 of operation mentioned above in the configuration which advances an authentication request.
[0043] gestalt 3. of operation -- with the gestalt 3 of this operation, in drawing 2 and drawing 11 which gave the same sign to the corresponding point with drawing 8 , when the personal authentication information specified by authentication information acquisition S/W11 transmitted from the authentication server 3 does not suit a user's intention, the procedure (SP2B, SP12A) in which a user refuses applicable authentication information acquisition S/W is shown. The authentication server terminal 3 with which acquisition was refused reselects other authentication information acquisition S/W (SP20A). However, it is the case where there is other authentication information acquisition S/W which can reselect as mentioned above about drawing 4 .
[0044] When accompanied by a thing and dysphoria with the specified biometrics acquisition equipment 6 dirty when using biometrics as individual authentication information, a user does refusal. Although biometrics is effective in identifying an individual, the problem of privacy

protection and the opportunity for a user to also refuse or change a sanitary problem for a certain reason are indispensable as mentioned above.
[0045] Moreover, also when biometrics acquisition equipment 6 cannot trust it in security, even if there is the intention to say that he wants to specify alternative means, such as a one-time password (OTP), even if complicated [other than biometrics information] and it follows the intention of refusal of a user or modification, the effectiveness that the existence of specification of an individual and this individual's access privilege can be certainly judged according to the environment can acquire by choosing authentication information acquisition S/W which acquires information dynamically required for authentication.
[0046] As a means to acquire the same effectiveness as the gestalt 3 of gestalt 4. implementation of operation, the optional feature of acquisition authentication information is included in authentication information acquisition S/W of the gestalten 1 and 2 of operation itself. In the example of the gestalt 1 of operation, what carries out authentication implementation for the fingerprint and hand information on D, and the thing to attest only with the fingerprint of E can be chosen as authentication information acquisition S/W which can be chosen. At this time, the places to which authentication information acquisition S/W which an authentication server combines with the authentication information acquisition function of D and E both is transmitted differ.
[0047] The configuration and operations sequence of Web system 1 the very thing are the same as that of the gestalten 1 and 2 of operation. The screen image of authentication information acquisition S/W by the side of a user is shown in drawing 12 . A user chooses either from D/E and acquires his own [an authentication means and] authentication information. If it chooses any of the selection carbon buttons 12A and 12B of a screen they are, authentication information acquisition S/W will operate, and authentication information chosen actually is acquired. At the authentication server terminal 3, with the classification of the sent authentication information, it can judge whether it can attest in the group of the sent information, and the same effectiveness as the gestalt 3 of operation can be acquired.
[0048] Although the authentication information acquired by authentication information acquisition S/W was determined with the gestalten 1-4 of the gestalt 5. above-mentioned operation of operation, it is good even if like [which the authentication information acquired not on authentication information acquisition S/W but on a screen is shown]. For example, at the time of the count of authentication of the detail database of the gestalt 1 of operation, it is displayed that fingerprint information and hand information are sent to a screen. Thereby, a user operates the software which acquires authentication information spontaneously according to the displayed content, and sends the acquired authentication information to the authentication server terminal 3.
[0049] Moreover, you may make it display that the authentication information which was not shown concretely but was beforehand decided by the display is sent. In this case, the software with which a user acquires authentication information for all the authentication information beforehand notified in advance by storage of a user from the manager etc. to the user separately spontaneously is operated, and the acquired authentication information is sent to an authentication server. If it does in this way, the same effectiveness as the gestalt 1 of above-mentioned operation is realizable, but in a display, since a means to acquire serves as treatment like a password when sending the authentication information which was not shown concretely but was decided beforehand, security can be improved much more.
[0050] In addition, in the gestalten 1-4 of above-mentioned operation, in the Web server terminal

4, although the case where a user's personal authentication was performed was described, it is widely applicable [this invention] to the general control unit which needs a user's personal authentication like the close leaving terminal unit connected not only to this but to the network.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the configuration of the gestalt 1 of operation [the remote authentication system by this invention] of ******** of a Web system.
[Drawing 2] It is the timing chart with which explanation of the authentication processing in the Web system of drawing 1 is presented.
[Drawing 3] It is the graph with which explanation of the example 1 of the authentication information database in the authentication server terminal of drawing 1 is presented.
[Drawing 4] It is the graph with which explanation of the example 1 of the authentication information database in the authentication server terminal of drawing 1 is presented.
[Drawing 5] It is the graph with which explanation of the example 2 of the authentication information database in the authentication server terminal of drawing 1 is presented.
[Drawing 6] It is the graph with which explanation of the example 2 of the authentication information database in the authentication server terminal of drawing 1 is presented.
[Drawing 7] It is the graph with which explanation of the example 3 of the authentication information database in the authentication server terminal of drawing 1 is presented.
[Drawing 8] It is the timing chart with which explanation of authentication processing of the example 3 in the Web system of drawing 1 is presented.
[Drawing 9] It is the block diagram showing the configuration of the gestalt 2 of operation [the remote authentication system by this invention] of ******** of a Web system.
[Drawing 10] It is the timing chart with which explanation of the authentication processing in the Web system of drawing 9 is presented.
[Drawing 11] It is the timing chart with which explanation when refusal occurs as a gestalt 3 of implementation of the authentication processing in the Web system of drawing 1 is presented.
[Drawing 12] It is approximate line drawing with which explanation of the display screen of authentication information acquisition S/W is presented as a gestalt 4 of operation of the Web system of drawing 1 .
[Description of Notations]
1 Web System
2 Network
3 Authentication Server Terminal
3A Authentication control section
3B Authentication information database
3C Authentication information acquisition software pool
4 Web Server Terminal
4A Web server database
4B Authentication request section
4C Web server software
5 User Terminal
5A Browser
5B Authentication information acquisition software actuation

6 Biometrics Acquisition Equipment
7 Fingerprint Acquisition Equipment
8 Palm-Print Acquisition Equipment
9 Character Recognition Tablet
10 Retina Information Acquisition Equipment
11 Authentication Information Acquisition Software

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－224236

(43)公開日　平成11年(1999)８月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ

審査請求　未請求　請求項の数３　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－24225

(22)出願日　平成10年(1998)２月５日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　中村　浩
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　藤井　照子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　貞包　哲男
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(74)代理人　弁理士　宮田　金雄　（外２名）

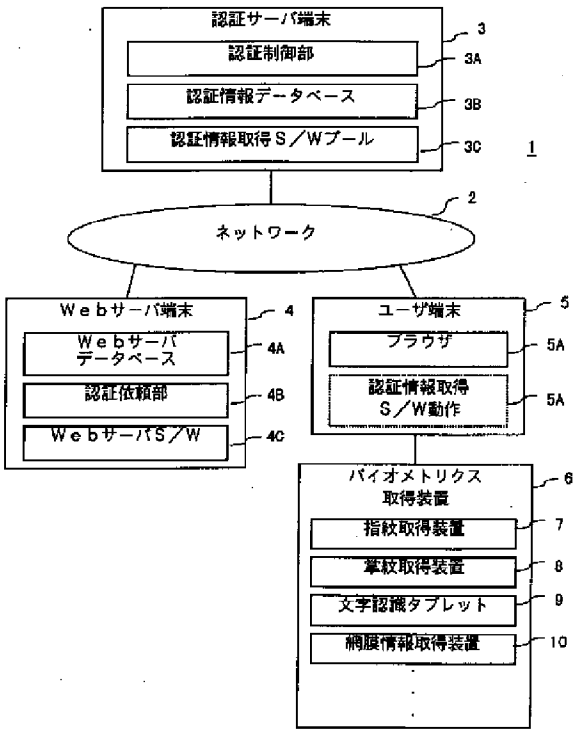
最終頁に続く

(54)【発明の名称】　遠隔認証システム

(57)【要約】

【課題】　遠隔認証システムにおいて、バイオメトリクス情報によりユーザの認証を行う際、確実にユーザの特定とアクセス件の有無を判定し得ると共に使い勝手を格段的に向上する。

【解決手段】　ユーザ端末には少なくとも１又は複数種類のバイオメトリクス取得装置が接続され、認証サーバにはユーザ端末及び又はユーザに応じた１又は複数の認証情報取得ソフトウェアが格納され、認証に際して認証サーバからダウンロードされるユーザ端末及び又はユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、１又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにした。



【特許請求の範囲】
【請求項１】　ネットワークに認証サーバと、認証クライアントと、ユーザ端末がそれぞれ接続され、上記ユーザ端末を通じて上記認証クライアントにアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも１又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた１又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記１又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたことを特徴とする遠隔認証システム。
【請求項２】　ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、上記ユーザ端末にアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも１又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた１又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記１又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたことを特徴とする遠隔認証システム。
【請求項３】　上記ユーザ端末に接続された上記複数のバイオメトリクス取得装置のうち、何れかを用いて上記バイオメトリクス情報として入力するかを上記ユーザが選択する手順を有する認証情報取得ソフトウェアを備えることを特徴とする請求項１又は請求項２に記載の遠隔認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、遠隔認証システムにおいて、バイオメトリクスにより個人の特定とその個人の情報やアプリケーションへのアクセス権の有無の判定を１つの認証サーバ端末にて集中的に行うシステムに関するものである。
【０００２】
【従来の技術】従来、ネットワークに接続された情報処理システムにおいて機密保持のため、個人を特定し該個人のアクセス許可と不許可の判断を行う、すなわち認証が必要である。また、銀行の現金自動支払い機等では個人の特定と預金残高等該個人の取り引き情報にアクセスするための認証や、機密度の高い研究場所や会員制クラブ等への入退室時にも個人の認証が実施されている。
【０００３】これらの認証として、身分証明書等と同様の位置づけである磁気カードやＩＣカード、パスワード等の個人の記憶や、これらの組み合わせによって個人の特定と資格の認定、すなわち認証を実施している。ところがパスワード等は忘却の恐れがあり、磁気カードやＩＣカード等は紛失や破壊等により認証が不能に陥ったり、盗難やパスワード情報の漏洩により本人以外が本人と成りすまして認証されてしまう等の問題がある。またこれらによって機密度を高く保つためには、確実に本人と認証する必要があるが、パスワード等を複雑にしたり、ワンタイムパスワード（ＯＴＰ）等の手段を用いると、その分記憶し難くなったり、認証操作自体が煩雑になる。さらに磁気カード等を使用しないで、記憶による認証を広域で実施（銀行の複数の店舗で使用）する場合には、認証情報は集中的に管理する必要がある。
【０００４】
【発明が解決しようとする課題】一方、指紋情報、掌紋情報、筆跡情報、網膜情報等の個人の生体的特徴であるバイオメトリクス情報による認証では、煩雑さを解消すると共に成りすましが困難である。バイオメトリクス情報による認証が広域で必要な場合には、上述と同様の理由及びプライバシー保護の面からも、集中的な管理と認証が必要である。このバイオメトリクス情報による認証を集中的に実施する場合、ユーザ毎だけではなく、認証を必要とするものや場所、システム等のセキュリティレベル（機密レベル）により適切な認証方法を選択して、認証情報を取得することが重要である。
【０００５】ここでＩＥＴＦ(Internet Engineering Task Force)のＲＦＣ（Request ForComment ）に登録されているＲＦＣ2138（ Remote Authentication Dial In User Service、以下ＲＡＤＩＵＳ、前ＲＦＣ2058が更新）で記述されているＲＡＤＩＵＳサーバは、ＲＡＤＩＵＳクライアントの認証要求を受け集中的に認証処理を行い認証結果を返送するが、認証手段や認証情報はユーザ毎に固定的に予め決められており、バイオメトリクス情報を取得する場合にはその取得環境に応じて動的に認証手段と認証情報を変更できないという問題があった。
【０００６】このような従来例として、さらに特開平９－８１５１８号公報に示される「ネットワーク上の認証方法」のように、ユーザホストがアプリケーションサーバにアクセスしてきた場合に、アプリケーションサーバが認証サーバに固定的な認証手段と認証情報を使用してユーザの認証を依頼し、認証結果を受けるような認証方法がある。
【０００７】またバイオメトリクス情報は個人を識別するのに有効であるが、プライバシー保護の問題と、バイオメトリクス取得装置自体が不潔なものや不快を伴う場合のように衛生的に取得上の問題もある。
【０００８】この発明は以上の問題点を解消するためなされたもので、バイオメトリクス情報により個人の認証を行う際、確実に個人の特定と該個人のアクセス件の有

無を判定し得ると共に使い勝手を格段的に向上し得る遠隔認証システム及び遠隔認証方法を得ることを目的とする。

【０００９】

【課題を解決するための手段】この発明に係る遠隔認証システムは、ネットワークに認証サーバと、認証クライアントと、ユーザ端末がそれぞれ接続され、上記ユーザ端末を通じて上記認証クライアントにアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも１又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた１又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記１又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたものである。

【００１０】また次の発明に係る遠隔認証システムは、ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、上記ユーザ端末にアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも１又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた１又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記１又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたものである。

【００１１】さらに次の発明に係る遠隔認証システムは、上記ユーザ端末に接続された上記複数のバイオメトリクス取得装置のうち、何れかを用いて上記バイオメトリクス情報として入力するかを上記ユーザが選択する手順を有する認証情報取得ソフトウェアを備えるものである。

【００１２】

【発明の実施の形態】以下図面を参照して、この発明の実施の形態について詳述する。

【００１３】実施の形態１．図１にこの発明をＷｅｂシステム１に適用した場合の実施の形態１の構成を示す。ネットワーク２上に認証サーバ端末３、認証クライアント端末４（本例ではＷｅｂサーバ端末）、ユーザ端末５等が接続される。このようなＷｅｂシステム１でＷｅｂサーバ４はユーザからユーザ端末５を通じてアクセスされた時に、そのユーザの個人認証を認証サーバ端末３から受け、その結果によりユーザに対してサービスを行う。

【００１４】認証サーバ端末３は、認証制御部３Ａと、認証情報データベース３Ｂと、認証情報取得ソフトウェアプール（以下、ソフトウェアは、Ｓ／Ｗと記述する）３Ｃとを格納するパーソナルコンピュータやワークステーション等のコンピュータ装置（以下、構成としてＣＰＵ、メモリ、ディスク、通信制御部等を有するものを示す）である。またＷｅｂサーバ端末４は、Ｗｅｂサーバデータベース４Ａと、認証依頼部４Ｂ及びユーザの認証が必要なＷｅｂサーバＳ／Ｗ４Ｃが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。

【００１５】ユーザ端末装置５は、Ｗｅｂサーバ端末４の情報を表示するブラウザ５Ａと、認証情報取得Ｓ／Ｗ５Ｂが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またユーザ端末装置５にはバイオメトリクス取得装置６が接続されている。バイオメトリクス取得装置６は、画像処理等により人体の指紋や掌紋情報をバイオメトリクス情報として取得する指紋取得装置７や掌紋取得装置８、ユーザが描いた筆跡情報をバイオメトリクス情報として取得する文字認識タブレット９、眼底スキャン等によって人体の網膜情報をバイオメトリクス情報として取得する網膜情報取得装置１０等を示している。

【００１６】このようなＷｅｂシステム１における認証処理の流れを図２に示す。まずユーザ端末装置５で動作しているアプリケーションであるブラウザ５Ａにより、ユーザが認証のクライアントであるＷｅｂサーバ端末４の機密度の高いＷｅｂサーバデータベース４Ａの情報にアクセスした場合（ＳＰ１）について説明する。その機密度の高い情報のアクセス制御を行っているアプリケーションであるＷｅｂサーバＳ／Ｗ４Ｃは、該ユーザがアクセス権限を有すか否かの判定するためにユーザ認証を行う必要がある（ＳＰ１０）。

【００１７】すなわちＷｅｂサーバ端末４のＷｅｂサーバＳ／Ｗ４Ｃは、クライアントＩＤ（認証依頼部の識別子）、アプリケーションＩＤ（認証を必要とするアプリケーションであるＷｅｂサーバＳ／Ｗ４Ｃの識別子）、アクセスデータ種別（ユーザがアクセスしてきたデータの機密レベル）と共に認証依頼部４Ｂにユーザの認証が必要であることを通知する（ＳＰ１１）。認証依頼部４Ｂは認証サーバ端末３へ上記情報を含むユーザの認証要求を送信する。

【００１８】ユーザの認証要求を受信した認証サーバ端末３の認証制御部３Ａは認証クライアントＩＤ、アプリケーションＩＤ、アクセスデータ種別から、認証情報取得Ｓ／Ｗ１１を選択する（ＳＰ２０）。認証情報取得Ｓ／Ｗ１１はそれぞれ取得する認証情報が決まっており、複数の認証情報を取得する認証情報取得Ｓ／Ｗ１１もある。認証制御部３Ａは選択した認証情報取得Ｓ／Ｗ１１を認証のクライアントであるＷｅｂサーバ端末４へ転送

する（ＳＰ２１）。

【００１９】ＷｅｂサーバＳ／Ｗ４Ｃに転送された認証情報取得Ｓ／Ｗ１１を引き渡し、ユーザから認証情報の取得を指示し、その指示によりＷｅｂサーバＳ／Ｗ４Ｃからユーザ端末５に認証情報取得Ｓ／Ｗ１１が転送される（ＳＰ１２）。

【００２０】ユーザ端末５のブラウザ５Ａは転送された認証情報取得Ｓ／Ｗ１１を受け取り、この認証情報取得Ｓ／Ｗ１１を認証情報Ｓ／Ｗ５Ｂとしてを動作させる（ＳＰ２）。認証情報Ｓ／Ｗは、自発的にユーザＩＤ（名前、会社、社員番号、所属、住所、電話等や、システムで個人毎に割り振られているＩＤ）の取得と、指紋情報、掌紋情報、筆跡情報、網膜情報等のバイオメトリクス情報や、パスワードやワンタイムパスワード等の従来のコンピュータシステムで通常使用される認証情報を取得する。このとき認証情報を取得するドライバ等の他のＳ／Ｗと協調して動作する場合もある。認証情報取得Ｓ／Ｗ５Ｂは、ブラウザ５Ａを介してＷｅｂサーバ端末へ取得したユーザＩＤと認証情報を転送する（ＳＰ３）。

【００２１】Ｗｅｂサーバ端末４の認証依頼部４ＢはＷｅｂサーバＳ／Ｗ４Ｃを介して、ユーザから取得したユーザＩＤと認証情報を認証サーバ端末３へ転送する（ＳＰ１３）。認証サーバ端末３の認証制御部３Ａは転送されたユーザＩＤと認証情報により、ユーザ認証を実施する（ＳＰ２２）。このとき転送されたバイオメトリクス情報等の認証情報は、認証サーバ端末３の認証情報データベース３Ｂに元々蓄積されている個人情報と照合する。転送された全ての認証情報の照合で本人と判断した場合には、この結果を認証のクライアントであるＷｅｂサーバ端末に通知する。また、照合結果が１つでも正しくなければ本人ではないと判断しこれを通知する（ＳＰ２３）。

【００２２】認証結果を受けた認証のクライアントであるＷｅｂサーバ端末４の認証依頼部４Ｂは、その認証結果をＷｅｂサーバＳ／Ｗ４Ｃに通知する。ＷｅｂサーバＳ／Ｗ４Ｃは該認証結果により該ユーザに対してＷｅｂサーバデータベースの機密度の高い情報へのアクセス許可又は不許可を判定する（ＳＰ１４）。例えば、該機密情報の表示を行う等、ユーザアクセスに対する動作を行う。

【００２３】なおユーザ端末５（認証情報取得Ｓ／Ｗ５Ｂ）とＷｅｂサーバ端末４間と、Ｗｅｂサーバ端末４と認証サーバ端末３間（認証制御部３Ａ）は暗号化すれば認証情報の秘匿を行えると共に、成りすましの脅威を減ずることができる。また個別端末間ではなく、ユーザ端末５（認証情報取得Ｓ／Ｗ５Ｂ）と認証サーバ端末３間（認証制御部３Ａ）で暗号化を実施しても同様に成りすましの脅威を減ずることができる。

【００２４】実施例１．ここで図３、図４を用いて、データベース構造の単純な例と認証情報取得Ｓ／Ｗ５Ｂの選択処理について説明する。図３の認証情報データベース３Ｂには個人ユーザ毎の情報として、ユーザＩＤ、ユーザレベル、認証情報の項目が格納されている。ユーザＩＤは、名前、会社、社員番号、所属、住所、電話等や、システムで個人毎に割り振られているＩＤである。またユーザレベルは機密情報へのアクセスレベルであり、さらに認証情報は照合元の認証情報としての指紋情報、筆跡情報、網膜情報等のバイオメトリクス情報、パスワード情報やワンタイムパスワードの情報等である。

【００２５】図４の認証情報取得Ｓ／Ｗプール３Ｃには、指紋情報と網膜情報の両方を取得する認証情報取得Ｓ／Ｗ１１や、２本の指紋情報を取得する認証情報取得Ｓ／Ｗ１１、指紋情報と筆跡情報を取得する認証情報取得Ｓ／Ｗ１１等が格納されている。また、認証情報取得Ｓ／Ｗプール３Ｃは、機密レベルに対応した選択可能な認証情報取得Ｓ／Ｗ１１とデータ種別が示されている。

【００２６】この実施例１での認証サーバ端末３の認証情報取得Ｓ／Ｗ１１の選択機構の説明として、まずデータ種別＝17のＷｅｂサーバデータベース４Ｃの情報にユーザがアクセスをしてきた場合を例とする。このとき認証依頼部４Ｂの識別子に相当する認証クライアントＩＤ＝15とし、ＷｅｂサーバＳ／Ｗ４Ｃの識別子に相当するアプリケーションＩＤ＝25とする。ＷｅｂサーバＳ／Ｗ４Ｃはデータ種別＝17にアクセス発生時、認証依頼部４Ｂにユーザの認証が必要であることを通知する。認証依頼部４Ｂは認証サーバ端末３へ上記情報、データ種別＝17、認証クライアントＩＤ＝15、アプリケーションＩＤ＝25を含むユーザの認証要求を送信する。そしてこれらの情報を含んだ認証要求を認証サーバ端末３が受信する。

【００２７】認証サーバ端末３の認証制御部３Ａは、図４の認証情報取得Ｓ／Ｗプール３Ｃのデータベースと受信した認証要求のデータ種別から要求されたデータは機密度レベル２であるため、図示のようにレベル２以上の認証情報取得Ｓ／Ｗ１１の選択可能候補を知る。

【００２８】実施例２．また図５及び図６を用いて、図３と同様に認証情報データベースの一部の別の実施例を説明する。ここには、認証クライアントＩＤ毎やアプリケーションＩＤ毎の選択可能な認証情報取得Ｓ／Ｗ１１が示されている。認証サーバ端末３の認証制御部３Ａは、これらの情報により、認証クライアントＩＤから選択できかつアプリケーションＩＤから選択できる認証情報取得Ｓ／Ｗ１１の候補を知る。従って、データ種別によって、Ａ、Ｂ、Ｃ、Ｄ、Ｅ、Ｆが候補になり、認証クライアントＩＤによって、Ｃ、Ｄ、Ｅが候補になり、アプリケーションＩＤによって、Ａ、Ｄ、Ｅ、Ｆが候補になり、最終的にＤ、Ｅのどちらかが選択される。

【００２９】この選択可能認証情報取得Ｓ／Ｗの候補か

らの認証サーバ端末３がランダムに選択、または固定的に決まったＳ／Ｗを選択、または順次選択といった手段で選択する。この例のように、アクセス情報であるデータ種別や、認証のクライアントである装置で動作している認証依頼部４Ｂや、使用アプリケーションであるＷｅｂサーバＳ／Ｗ４Ｃ等の環境に応じて認証手段と認証情報をフレキシブルに選択でき、個人の特定と該個人のアクセス権の有無を環境に応じて確実に判定できる。

【００３０】実施例３．次の実施例として、ユーザＩＤが認証要求に含まれており、図３の認証情報データベースが図７に示すように詳細設定されている場合を説明する。この処理の流れを図２との対応部分に同一符号を付した図８に示す。まず、Ｗｅｂサーバ端末４は、ユーザＩＤ（名前、会社、社員番号、所属、住所、電話等やシステムで個人毎に割り振られているＩＤ）を取得し、取得したユーザＩＤ、クライアントＩＤ（認証依頼部４Ｂの識別子）、アプリケーションＩＤ（認証を必要とするアプリケーションであるＷｅｂサーバＳ／Ｗ４Ｃの識別子）、アクセスデータ種別（ユーザがアクセスしてきたデータの機密レベル）とともに認証依頼部４Ｂに該ユーザの認証を依頼する。

【００３１】図７の認証情報データベース３Ｂは、ユーザの種別（データ管理者か一般ユーザか等）、使用できる認証クライアントＩＤ、使用できるアプリケーションＩＤ、本人と認証された場合にアプリケーションに引き渡されるアプリケーションの制御情報、照合ログとして過去の規定認証回数までの認証情報取得Ｓ／Ｗの選択状況と照合率、総認証回数、選択基準等、ユーザ個人毎の情報が図３の認証情報データベースに追加されている。

【００３２】ユーザＩＤが認証要求に含まれている場合には、図７の該当ユーザの選択基準に従って選択する。具体例としてユーザＩＤ＝１であり、他は前の例と同様にデータ種別＝17、認証クライアントＩＤ＝15、アプリケーションＩＤ＝25の場合、認証依頼部４Ｂは認証サーバ端末３へ、上記情報としてユーザＩＤ＝１、データ種別＝17、認証クライアントＩＤ＝15、アプリケーションＩＤ＝25を含むユーザの認証要求を送信する。

【００３３】そしてこれらの情報を含んだ認証要求を認証サーバ端末３が受信する。上述と同様にデータ種別によってＡ、Ｂ、Ｃ、Ｄ、Ｅ、Ｆが候補になり、認証クライアントＩＤによってＣ、Ｄ、Ｅが候補になり、アプリケーションＩＤによってＡ、Ｄ、Ｅ、Ｆが候補になり、最終的にＤ、Ｅのどちらかが選択される。また、ユーザＩＤ＝１であることから、認証制御部３Ａは総認証回数によって選択を実施する。総認証回数の１回目はＤ、２回目はＥ３回目はＤ、４回目Ｅ……というように選択する。ここではユーザＩＤ＝１の総認証回数＝20で、今回は21回目であるため認証情報取得Ｓ／Ｗ１１のＤが選択される。

【００３４】他の実施例．また、図７に示すように認証情報データベース３Ｂにユーザ毎に使用できる認証クライアントＩＤ、使用できるアプリケーションＩＤに指定があれば、指定された認証クライアントやアプリケーションを使用しているときのみ該ユーザに対して認証情報取得Ｓ／Ｗ１１を送付する等のアクセス制御が実現できる。ここでは、使用できるクライアントＩＤに15があり、使用できるアプリケーションＩＤにも25があるため、認証情報取得Ｓ／Ｗ１１の送付が許可される。

【００３５】また、図７に示すユーザ種別によっても認証情報取得Ｓ／Ｗ１１の送付の可否を判定できる。さらに認証クライアントやアプリケーションにユーザと同様に機密レベルを割り振れば、認証情報取得Ｓ／Ｗ１１の選択時に、認証サーバ端末３は認証クライアントのレベルとアプリケーションのレベルとアクセスデータ種別のレベルから認証情報取得Ｓ／Ｗ１１を選択できる。すなわち、例えば３つの中の最も高いレベル以上の認証情報取得Ｓ／Ｗ１１から選択するような制御ができる。

【００３６】認証情報取得Ｓ／Ｗ１１の送付以降は、上述と同様であるが、ユーザＩＤはすでに取得しているため、認証情報のみが転送されるところが異なる。また、図７の本人と認証された場合にアプリケーションに引き渡されるアプリケーションの制御情報である、Ｋｅｙ－１をＷｅｂサーバ端末４が使用して多彩なアクセス制御を実現することもできる。

【００３７】さらに、選択基準が図７の照合率の例として、上述では選択基準が総認証回数であったが、これに代え、選択基準が照合評価とした場合には、レベル２以上の認証情報取得Ｓ／Ｗ１１の中で、過去の照合評価の最も高いものを該ユーザの照合ログから探し、それを選択する。ここでは前回のＥの照合評価が最も高いのでＥが選択される。

【００３８】また、認証サーバ端末３から認証クライアントへの認証取得Ｓ／Ｗ転送を省略する例もある。上述したＷｅｂシステム１のケースでは認証クライアントであるＷｅｂサーバ端末４によって、認証情報取得Ｓ／Ｗが固定的に決まってしまう場合には、認証クライアントのＷｅｂサーバ端末４が認証情報取得Ｓ／Ｗ１１を予め取得しておき、その認証情報取得Ｓ／Ｗ１１を認証サーバ端末３から認証クライアントのＷｅｂサーバ端末４へ、認証情報取得Ｓ／Ｗの転送なしにユーザ端末５に転送するようにしても良い。

【００３９】以上のように、このＷｅｂシステム１においては、バイオメトリクス情報により認証を行う場合に、アクセスしてきたユーザや、アクセス情報であるデータ種別や、認証のクライアントであるＷｅｂサーバ端末４で動作している認証依頼部４Ｂや、使用アプリケーションであるＷｅｂサーバＳ／Ｗ４Ｃ等の環境や認証履歴（認証時状態）に応じて、動的に認証に必要な情報を取得する認証情報取得Ｓ／Ｗ１１を選択することにより、個人の特定と該個人のアクセス権の有無をその環境

に応じて確実に判定できる。

【００４０】実施の形態２．この実施の形態２においては実施の形態１を簡略化したものである。図１との対応部分に同一符号を付した図９は、バイオメトリクス情報を取得するユーザ端末と認証クライアントの端末が同一である。認証が必要なアプリケーションの例としてデータベース検索を行うデータベース検索アプリケーション５Ｅがあり、データベース検索アプリケーション５Ｅが使用するローカルデータベース５Ｃ、認証依頼部５Ｄ、ユーザの認証が必要なデータベース検索アプリケーション５Ｅと認証情報取得Ｓ／Ｗ１１が動作するパーソナルコンピュータ、ワークステーション等のコンピュータ装置である。バイオメトリクス取得装置６はユーザ端末５に接続されており、上述した実施の形態１と全く同様の構成であり、また認証サーバ端末３も、上述した実施の形態１と全く同様の構成である。

【００４１】基本的には上述の実施の形態１と同じであり、図２、図８との対応部分に同一符号を付した図１０において、データベース検索アプリケーション５Ｅは、ローカルデータベース５Ｃの機密情報へアクセスする際に（ＳＰ５）、まずユーザＩＤ（名前、会社、社員番号、所属、住所、電話等や、システムで個人毎に割り振られているＩＤ）を取得し（ＳＰ６）、取得したユーザＩＤ、クライアントＩＤ（認証依頼部５Ｄの識別子）、アプリケーションＩＤ（認証を必要とするアプリケーションであるデータベース検索アプリケーション５Ｅの識別子）、アクセスデータ種別（ユーザがアクセスしてきたデータの機密レベル）と共に、認証依頼部５Ｄに該ユーザの認証を依頼する（ＳＰ７）。

【００４２】認証サーバ端末３の動作は実施の形態１と同じであり、認証処理を実行し認証結果を受けた認証のクライアントであるユーザ端末５の認証依頼部５Ｄは、その認証結果をデータベース検索アプリケーション５Ｅに通知する。データベース検索アプリケーション５Ｅは該認証結果により、該ユーザに対してローカルデータベース５Ｃの機密度の高い情報へのアクセスを許可するか否かを判定する（ＳＰ８）。例えば該機密情報の表示を行う等、ユーザアクセスに対する動作を行う。このような構成によれば、ユーザ端末５が認証リクエストを出す構成において、上述した実施の形態１と同一の効果を得ることができる。

【００４３】実施の形態３．この実施の形態３では、図２、図８との対応部分に同一符号を付した図１１において、認証サーバ３から転送されてきた認証情報取得Ｓ／Ｗ１１が指定する個人認証情報がユーザの意向に合わない場合、ユーザが該当認証情報取得Ｓ／Ｗを拒否する手順（ＳＰ２Ｂ、ＳＰ１２Ａ）を示す。取得が拒否された認証サーバ端末３は、他の認証情報取得Ｓ／Ｗを再選択する（ＳＰ２０Ａ）。ただし、図４について上述したように再選択できる認証情報取得Ｓ／Ｗが他にある場合である。

【００４４】バイオメトリクスを個人の認証情報として使用する場合には、指定されたバイオメトリクス取得装置６が不潔なものや不快を伴う場合に、ユーザが拒否ができる必要がある。バイオメトリクスは個人を識別するのに有効であるが、プライバシー保護の問題と上記のように衛生上の問題もあるため、ユーザが拒否又は変更できる機会が必須である。

【００４５】またバイオメトリクス取得装置６がセキュリティ的に信用できない場合も、バイオメトリクス情報以外の煩雑ではあってもワンタイムパスワード（ＯＴＰ）等の代替え手段を指定したいという意向があり、ユーザの拒否又は変更の意向に従っても、動的に認証に必要な情報を取得する認証情報取得Ｓ／Ｗを選択することにより、個人の特定と該個人のアクセス権の有無をその環境に応じて確実に判定できる効果を得られる。

【００４６】実施の形態４．実施の形態３と同様の効果を得る手段として、実施の形態１、２の認証情報取得Ｓ／Ｗ自体に取得認証情報の選択機構が含まれる。実施の形態１の例では選択できる認証情報取得Ｓ／ＷにはＤの指紋と筆跡情報で認証実施するものと、Ｅの指紋のみで認証するものが選択できる。このとき認証サーバはＤとＥ両方の認証情報取得機能を兼ね備えた認証情報取得Ｓ／Ｗを転送するところが異なる。

【００４７】Ｗｅｂシステム１自体の構成や動作手順は、実施の形態１、２と同様である。ユーザ側での認証情報取得Ｓ／Ｗの画面イメージを図１２に示す。ユーザはＤ／Ｅからどちらかを選択して、認証手段と自分自身の認証情報の取得を行う。画面の選択ボタン１２Ａ、１２Ｂの何れかを選択すると認証情報取得Ｓ／Ｗが動作して、実際に選択された認証情報の取得を行う。認証サーバ端末３では送られてきた認証情報の種別と共に、送られてきた情報の組で認証可能かを判断でき、実施の形態３と同様の効果を得ることができる。

【００４８】実施の形態５．上述の実施の形態１～４では、認証情報取得Ｓ／Ｗによって取得する認証情報が決定されていたが、認証情報取得Ｓ／Ｗではなく画面に取得する認証情報が示されるだけのようにしても良い。例えば実施の形態１の詳細データベースの認証回数の時には、画面に指紋情報と筆跡情報を送るように表示する。これによりユーザは表示された内容に従い自発的に認証情報を取得するソフトウエア等を動作させて、取得した認証情報を認証サーバ端末３に送る。

【００４９】また、表示で具体的に示されず、予め決められた認証情報を送付するよう表示するようにしても良い。この場合はユーザの記憶によって予め事前に別途ユーザに対して、管理者等から通知されている全ての認証情報を、ユーザは自発的に認証情報を取得するソフトウエア等を動作させて、取得した認証情報を認証サーバに送る。このようにすれば上述の実施の形態１と同様の効

果を実現できるが、表示では具体的に示されず予め決められた認証情報を送付する場合に、取得する手段がパスワード的な扱いとなるため、セキュリティを一段と向上できる。

【００５０】なお上述の実施の形態１～４においては、Ｗｅｂサーバ端末４において、ユーザの個人認証を行う場合について述べたが、この発明はこれに限らず、例えばネットワークに接続された入退室端末装置等のように、ユーザの個人認証が必要な制御装置一般に広く適用できる。

【００５１】

【発明の効果】上述の通りこの発明によれば、認証サーバは、バイオメトリクス情報により認証を行う際に、ユーザのバイオメトリクス情報の取得環境に応じて、バイオメトリクス取得装置と認証情報を自由に選択し取得するができ、かくして確実にユーザの特定とそのユーザのアクセス権の有無を判定し得る遠隔認証システムを実現できる。

【００５２】またユーザは指定された認証情報の取得について不満があった場合に、取得する認証情報を変更や拒否することができ、バイオメトリクス取得装置が不潔等で不快感を伴う場合やバイオメトリクス情報を取得する装置が信頼できない場合でも、代替手段で確実にかくして確実にユーザの特定とそのユーザのアクセス権の有無を判定できる。

【図面の簡単な説明】

【図１】　この発明による遠隔認証システムを適用したをＷｅｂシステムの実施の形態１の構成を示すブロック図である。

【図２】　図１のＷｅｂシステムにおける認証処理の説明に供するタイミングチャートである。

【図３】　図１の認証サーバ端末における認証情報データベースの実施例１の説明に供する図表である。

【図４】　図１の認証サーバ端末における認証情報データベースの実施例１の説明に供する図表である。

【図５】　図１の認証サーバ端末における認証情報データベースの実施例２の説明に供する図表である。

【図６】　図１の認証サーバ端末における認証情報データベースの実施例２の説明に供する図表である。

【図７】　図１の認証サーバ端末における認証情報データベースの実施例３の説明に供する図表である。

【図８】　図１のＷｅｂシステムにおける実施例３の認証処理の説明に供するタイミングチャートである。

【図９】　この発明による遠隔認証システムを適用したをＷｅｂシステムの実施の形態２の構成を示すブロック図である。

【図１０】　図９のＷｅｂシステムにおける認証処理の説明に供するタイミングチャートである。

【図１１】　図１のＷｅｂシステムにおける認証処理の実施の形態３として拒否が発生した場合の説明に供するタイミングチャートである。

【図１２】　図１のＷｅｂシステムの実施の形態４として認証情報取得Ｓ／Ｗの表示画面の説明に供する略線図である。

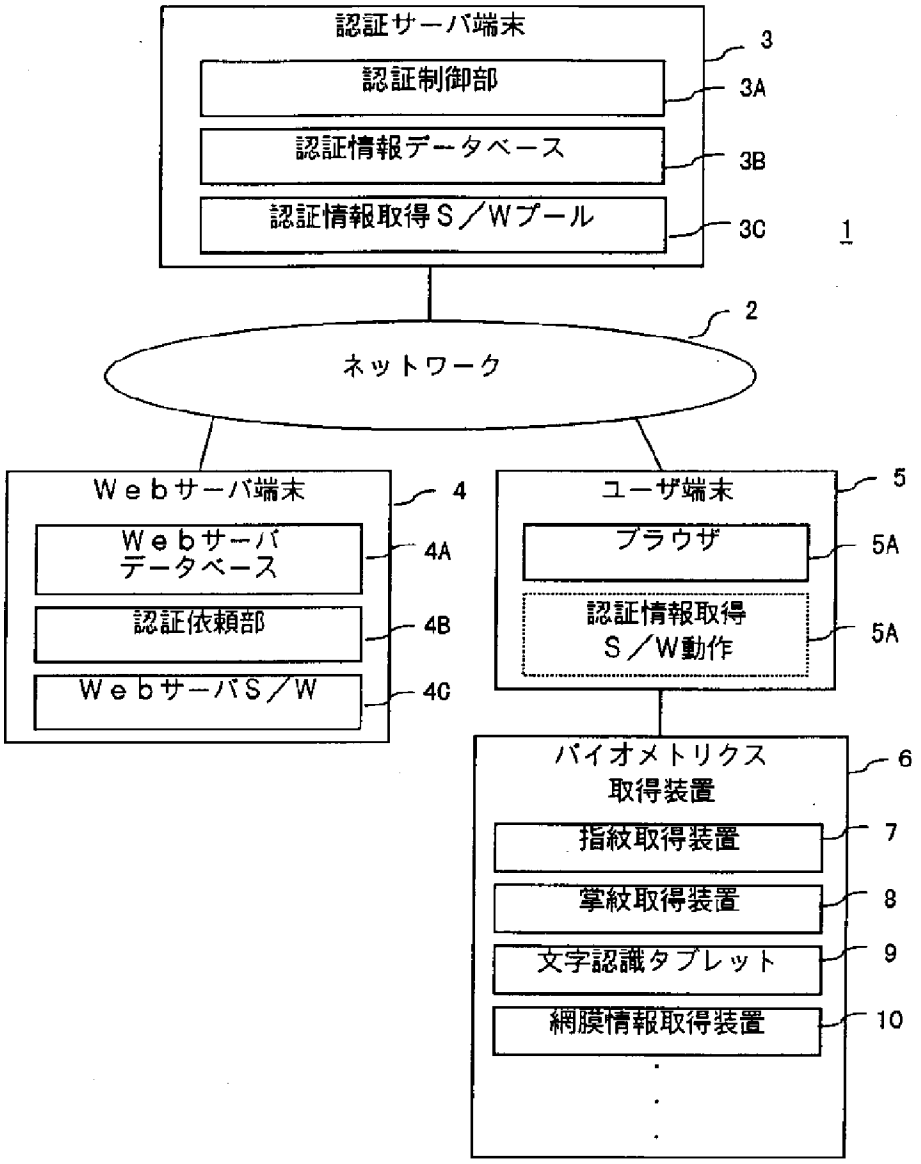
【符号の説明】

１　Ｗｅｂシステム
２　ネットワーク
３　認証サーバ端末
３Ａ　認証制御部
３Ｂ　認証情報データベース
３Ｃ　認証情報取得ソフトウェアプール
４　Ｗｅｂサーバ端末
４Ａ　Ｗｅｂサーバデータベース
４Ｂ　認証依頼部
４Ｃ　Ｗｅｂサーバソフトウェア
５　ユーザ端末
５Ａ　ブラウザ
５Ｂ　認証情報取得ソフトウェア動作
６　バイオメトリクス取得装置
７　指紋取得装置
８　掌紋取得装置
９　文字認識タブレット
１０　網膜情報取得装置
１１　認証情報取得ソフトウェア

【図３】

ユーザ ID	1｛名前、会社、社員番号、所属、住所、電話、など｝	2	・・・	・・・
ユーザレベル	2			
認証情報	｛指紋 1、指紋２、筆跡、網膜、パスワード、ワンタイムパスワード情報｝			

【図１】



【図４】

レベル	データ種別	認証情報取得Ｓ／Ｗ
1（最高機密）	1～10	A，B，C
2	11～20	D，E，F
3	21～30	G，H

A：指紋と網膜
B：指紋2指
C：網膜と筆跡
D：指紋と筆跡
E：指紋
F：筆跡
G：ワンタイムパスワード
H：パスワード

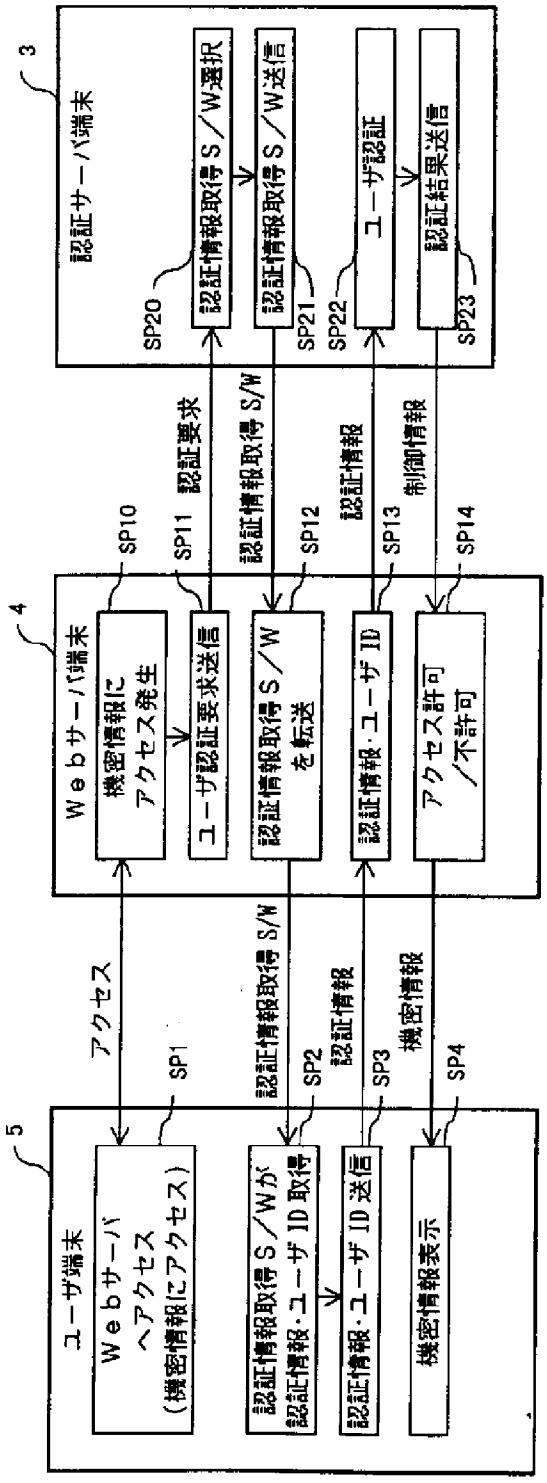
【図５】

認証クライアントID	認証情報取得Ｓ／Ｗ
	E，F
15	C，D，E
	A，B，C
	D，E，F
	G，H

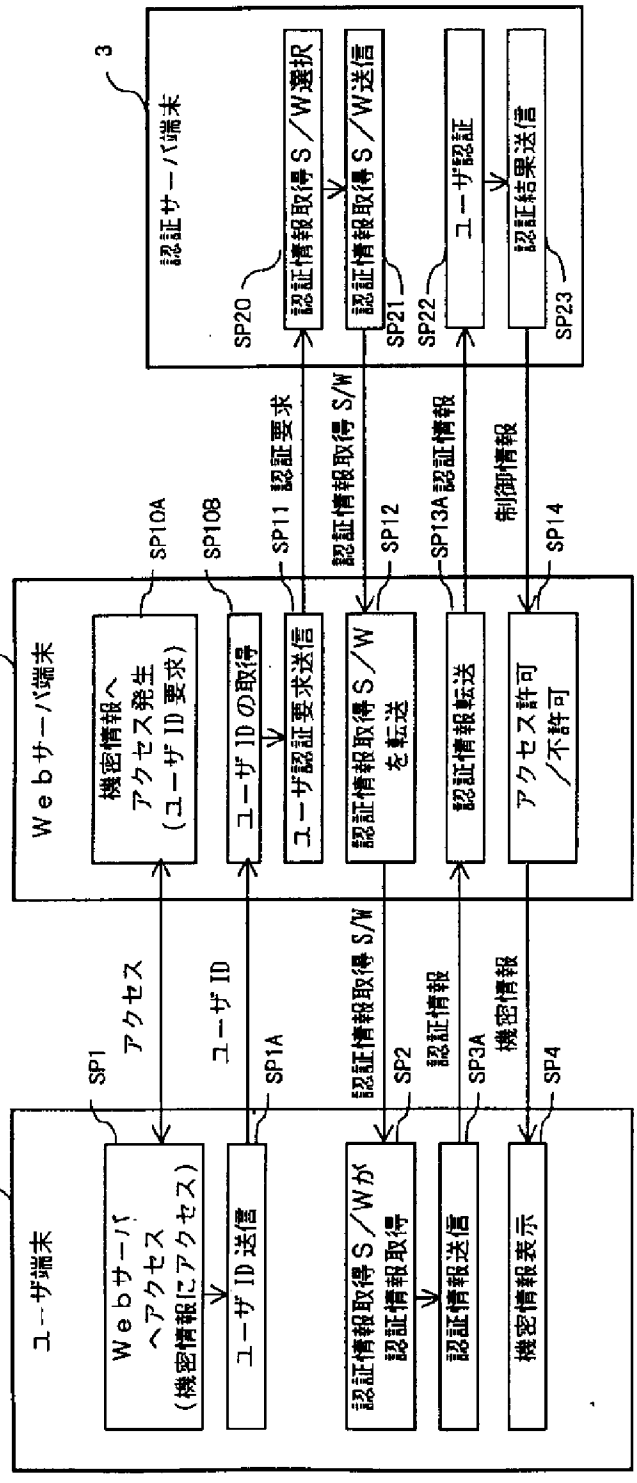
【図６】

アプリケーションID	認証情報取得Ｓ／Ｗ
	C，E，G
25	A，D，E，F
	E，F
	G，H

【図２】


3
認証サーバ端末
SP20
認証情報取得Ｓ／Ｗ選択
SP21
認証情報取得Ｓ／Ｗ送信
SP22
ユーザ認証
認証結果送信
SP23
4
Ｗｅｂサーバ端末
SP10
機密情報にアクセス発生
SP11 認証要求
ユーザ認証要求送信
認証情報取得 S/W
認証情報取得Ｓ／Ｗを転送
SP12
認証情報
認証情報・ユーザ ID
SP13
制御情報
アクセス許可／不許可
SP14
5
ユーザ端末
アクセス
SP1
Ｗｅｂサーバへアクセス（機密情報にアクセス）
認証情報取得 S/W
SP2
認証情報
認証情報取得Ｓ／Ｗが認証情報・ユーザ ID 取得
SP3
機密情報
認証情報・ユーザ ID 送信
SP4
機密情報表示

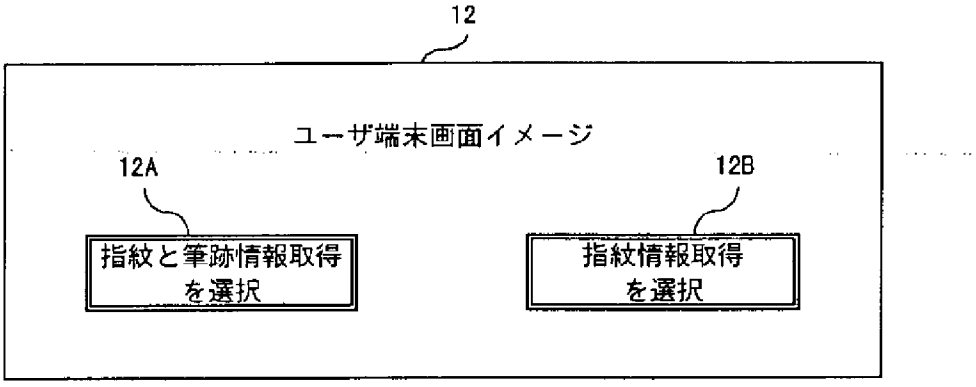
【図８】


3
認証サーバ端末
SP20
認証情報取得Ｓ／Ｗ選択
SP21
認証情報取得Ｓ／Ｗ送信
SP22
ユーザ認証
認証結果送信
SP23
4
Ｗｅｂサーバ端末
SP10A
機密情報へアクセス発生（ユーザ ID 要求）
SP10B
ユーザ ID の取得
SP11 認証要求
ユーザ認証要求送信
認証情報取得 S/W
認証情報取得Ｓ／Ｗを転送
SP12
SP13A 認証情報
認証情報転送
制御情報
アクセス許可／不許可
SP14
5
ユーザ端末
SP1
アクセス
Ｗｅｂサーバへアクセス（機密情報にアクセス）
ユーザ ID
SP1A
ユーザ ID 送信
認証情報取得 S/W
認証情報取得Ｓ／Ｗが認証情報取得
SP2
認証情報
SP3A
認証情報送信
機密情報
SP4
機密情報表示

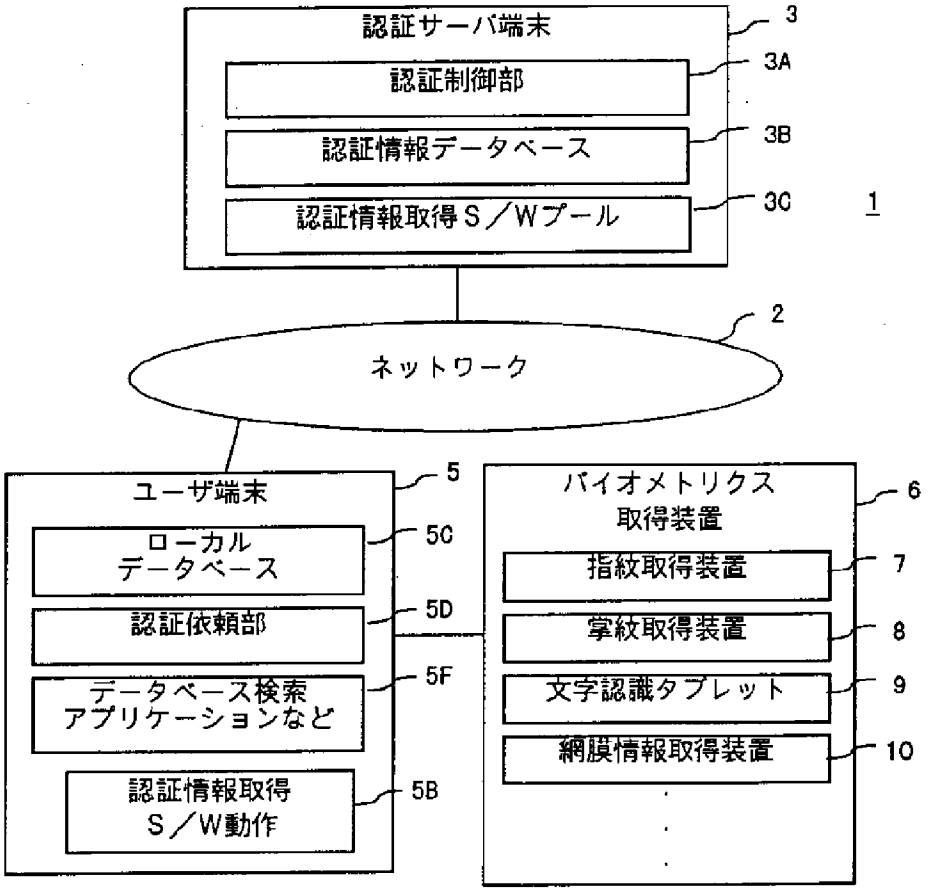
【図７】

ユーザ ID	1 {名前、会社、社員番号、所属、住所、電話、など}	2	・・・	・・・
ユーザ種別	一般			
ユーザレベル	2			
使用できるクライアント ID	10,15			
使用できるアプリケーション ID	8,25,36			
アプリケーション制御情報	key-1			
認証情報	{指紋 1、指紋 2、 筆跡、網膜、パスワード、ワンタイムパスワード情報}			
照合ログ	前回　：認証情報取得 S／W　E選択, 照合評価 90%, 指紋 1=90% 前々回：認証情報取得 S／W　D選択, 照合評価 75% 指紋 2=80%, 筆跡=70% ・ ・ ・			
総認証回数	20			
選択基準	総認証回数（他例：照合率）			

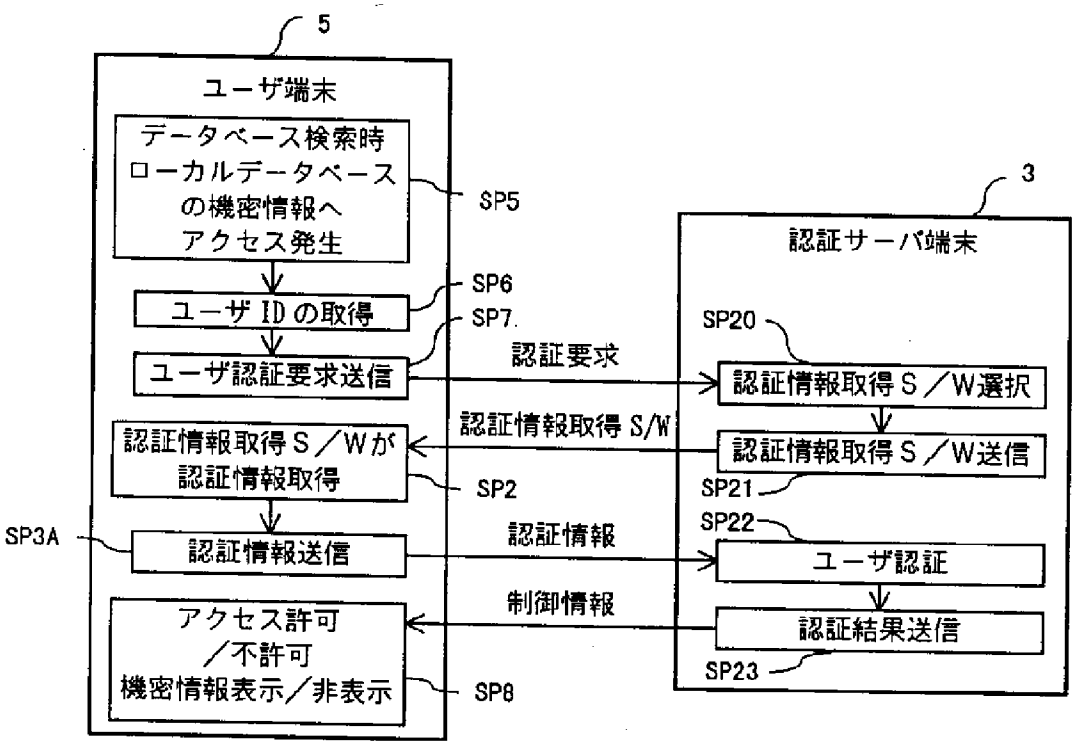
【図１２】



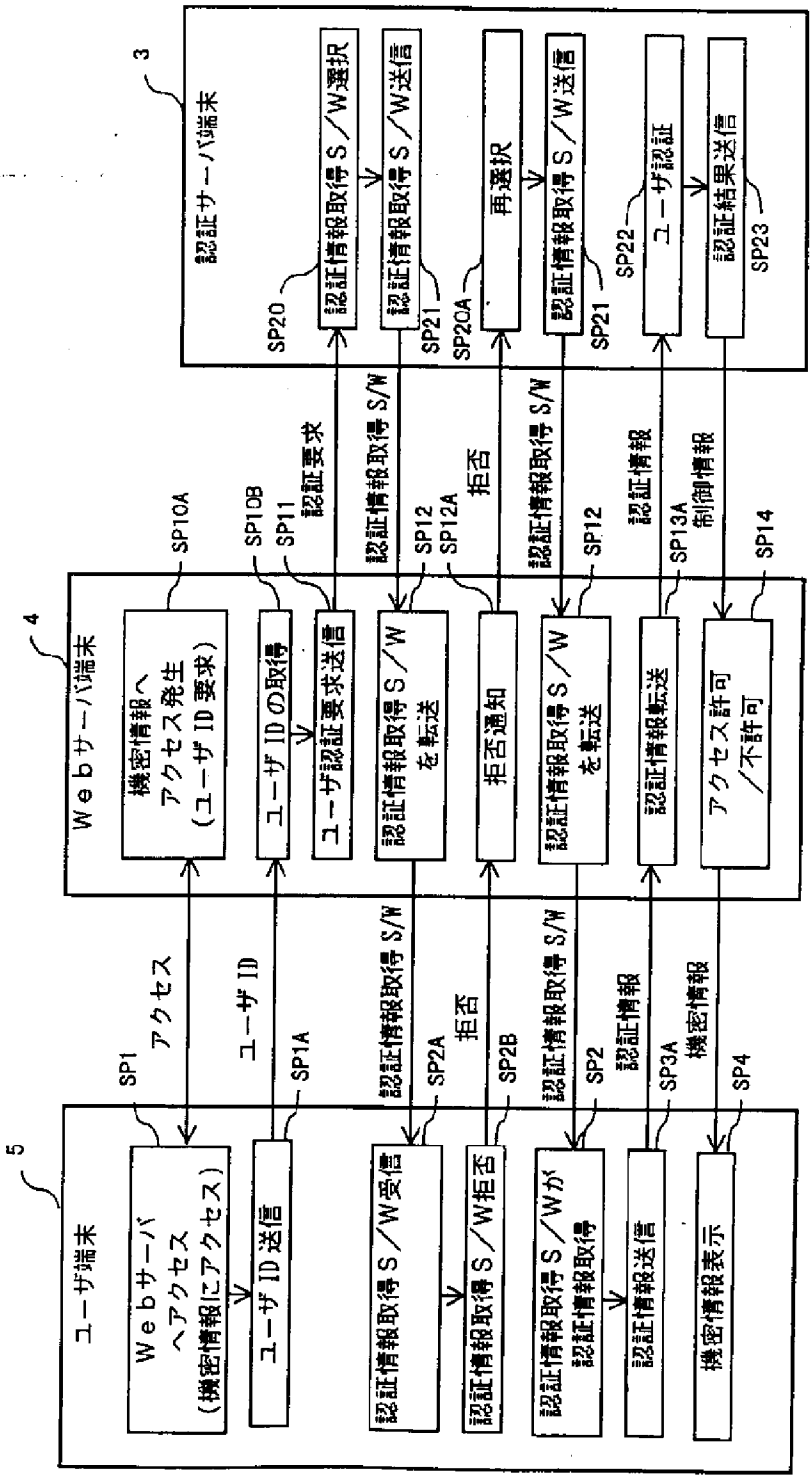
【図９】


認証サーバ端末
3
認証制御部
3A
認証情報データベース
3B
認証情報取得Ｓ／Ｗプール
3C
1
2
ネットワーク
ユーザ端末
5
ローカル
データベース
5C
認証依頼部
5D
データベース検索
アプリケーションなど
5F
認証情報取得
Ｓ／Ｗ動作
5B
バイオメトリクス
取得装置
6
指紋取得装置
7
掌紋取得装置
8
文字認識タブレット
9
網膜情報取得装置
10

【図１０】


5
ユーザ端末
データベース検索時
ローカルデータベース
の機密情報へ
アクセス発生
SP5
SP6
ユーザ ID の取得
SP7
ユーザ認証要求送信
認証要求
3
認証サーバ端末
SP20
認証情報取得 S ／W選択
認証情報取得 S/W
認証情報取得 S ／W送信
SP21
認証情報取得 S ／W が
認証情報取得
SP2
SP3A
認証情報送信
認証情報
SP22
ユーザ認証
制御情報
認証結果送信
SP23
アクセス許可
／不許可
機密情報表示／非表示
SP8

【図１１】


3
認証サーバ端末
SP20
認証情報取得Ｓ／Ｗ選択
SP21
認証情報取得Ｓ／Ｗ送信
SP20A
再選択
SP21
認証情報取得Ｓ／Ｗ送信
SP22
ユーザ認証
SP23
認証結果送信
4
Ｗｅｂサーバ端末
SP10A
機密情報へアクセス発生（ユーザＩＤ要求）
SP10B
ユーザＩＤの取得
SP11
ユーザ認証要求送信
認証要求
認証情報取得Ｓ／Ｗ
SP12
認証情報取得Ｓ／Ｗを転送
SP12A
拒否通知
拒否
認証情報取得Ｓ／Ｗ
SP12
認証情報取得Ｓ／Ｗを転送
認証情報取得 S/W
認証情報転送
SP13A
制御情報
アクセス許可／不許可
SP14
5
ユーザ端末
SP1
Ｗｅｂサーバへアクセス（機密情報にアクセス）
アクセス
ユーザＩＤ送信
SP1A
ユーザＩＤ
認証情報取得Ｓ／Ｗ受信
SP2A
認証情報取得 S/W
認証情報取得Ｓ／Ｗ拒否
SP2B
拒否
認証情報取得Ｓ／Ｗが認証情報取得
SP2
認証情報取得 S/W
認証情報送信
SP3A
認証情報
機密情報表示
SP4
機密情報

フロントページの続き

(72)発明者　馬場　義昌
東京都千代田区丸の内二丁目２番３号　三
菱電機株式会社内